# JREEC

# Journal of Renewable Energy-Electronics and Control

e-ISSN 2807-2189

A Robust researcher media communication on electrical engineering development applied technology:


| JREEC | VOLUME 3 | NOMER 1 | HALAMAN 1- 67 | Juni 2023 | ISSN 2807-2189 |
|---|---|---|---|---|---|

Diterbitkan oleh:

Jurusan Teknik Elektro
Institut Teknologi Adhi Tama Surabaya

https://ejurnal.itats.ac.id/jreec

# JREEC

**Journal of Renewable Energy, Electronic and Control**

**Volume 03, Nomer 01, Juni 2023**



**Alamat Redaksi & Distribusi**

Jurusan Teknik Elektro
Fakultas Teknik Elektro dan Teknologi Informasi
Institut Teknologi Adhi Tama Surabaya
Jl. Arief Rachman Hakim 100 Surabaya 60117
Telp. (031) 5945043, 5946331
Fax. (031) 5994620

Email: jreec.journal@itats.ac.id
Url: http://ejurnal.itats.ac.id/index.php/jreec

**JREEC: Journal of Renewaable Energy, Elektronic and Control**

Diterbitkan oleh Jurusan Teknik Elektro, Fakultas Teknik Elektro dan Teknologi Informasi, Institut Teknologi Adhi Tama Surabaya. Jurnal ini memuat artikel dari hasil oenelitian ilmiah yang mencakup bidang :

- Electrical Engineering
- Power Engineering
- Control Techniques
- Telecommunications
- Electronics
- Renewable Energy
- Energy Conversion
- Artificial Intelligent
- Robotic
- Image Processing
- Video Processing

Jurnal ini diterbitkan selama 2 kali setahun pada bulan Mei dan September.

**JREEC**
**Journal of Renewaable Energy, Elektronic and Control**
**Volume 03, Nomer 01, 2023**

## DAFTAR ISI

JREEC
JOURNAL RENEWABLE ENERGY ELECTRONICS AND CONTROL
homepage URL : https://ejurnal.itats.ac.id/jreec

# APLIKASI DIAGNOSA PENYAKIT PADA BALITA MENGGUNAKAN SISTEM PAKAR DENGAN METODE FORWARD CHAINING BERBASIS WEBSITE

**Delta Khairunnisa [1], Dewi Irmawati.S[2], Devi Sartika[3], Ienda Meiriska[4], Alan Novi Tompunu[5], Aridinda[6]**
[1-4,6]Program Studi Manajemen Informatika,[5]Teknik Komputer
Politeknik Negeri Srwijaya Srijaya Negara Bukit Besar Palembang

**INFORMASI ARTIKEL**

Jurnal JREEC – Volume 03 Nomer 01, Juni 2023

Halaman:
1 – 8
Tanggal Terbit :
06 Juni 2023

DOI:
10.31284/j.JREEC.2023.v31i.4235

**EMAIL**

delta.khairunnisa@gmail.com
dewiirmawati@yahoo.com
devi_sartika_mi@polsri.ac.id
alan_nt@gmail.com

Jurusan Teknik Elektro-ITATS
Alamat:
Jl. Arief Rachman Hakim No.100,Surabaya 60117,
Telp/Fax: 031-5997244



***ABSTRACT***

In this study aims to provide information for diagnosing diseases in toddlers with the Forward Chaining Inference method so that the final results of this study are expected to get the right solution for the symptoms suffered by toddlers. System design using the Unified Modeling Language (UML). The tools used for building are xampp (App Server), while the programming language used is php and the CodeIgniter framework. The application in this study is expected to facilitate the process of diagnosing diseases in toddlers.

***Keywords:*** Applications, Inference Forward Chaining and Unified Modeling Language (UML).

**ABSTRAK**

Dalam penelitian ini bertujuan untuk memberikan informasi untuk mendiagnosa penyakit pada Balita dengan metode *Inferensi Forward Chaining* sehingga hasil akhir dari penelitian ini diharapkan dapat mendapatkan solusi yang tepat dari gejala yang di derita oleh balita. Perancangan sistem dengan menggunakan *Unified Modeling Language* (UML). *Tools* yang digunakan untuk membangun adalah *xampp (App Server), sedangkan* bahasa pemrograman yang digunakan adalah php dan *framework Codeigniter*. Aplikasi dalam penelitian ini diharapkan dapat mempermudah proses diagnosa penyakit pada Balita.

**Kata Kunci** : *Aplikasi*, *Inferensi Forward Chaining* dan *Unified ModelingLanguage* (UML).

## PENDAHULUAN

Sistem pakar merupakan program komputer yang meniru proses pemikiran dan pengetahuan pakar dalam menyelesaikan suatu masalah tertentu. Implementasi sistem pakar banyak digunakan dalam bidang kesehatan karena sistem pakar dipandang sebagai cara penyimpanan pengetahuan pakar pada bidang tertentu dalam program komputer sehingga keputusan dapat diberikan dalam melakukan penalaran secara cerdas.Bayi yang berada pada rentang usia 0-5 tahun atau biasa dikenal

dengan balita rentan terhadap kuman penyakit dan kurangnya kepekaan terhadap gejala suatu penyakit yang merupakan ketakutan tersendiri bagi orang tua balita tersebut. Terkadang ada orang tua yang belum mengetahui ilmu tentang kesehatan pada anak atau balita, sehingga apabila terjadi gangguan kesehatan pada balita, orang tua akan lebih mempercayakan pengobatan balita kepada dokter ahli yang sudah mengetahui lebih banyak penyakit tanpa mempertimbangkan apakah gangguan tersebut masih dalam tingkat rendah atau kronis. [2][3].

Namun dengan kemudahan dan adanya para pakar atau dokter ahli terkadang terdapat juga kelemahan seperti jam kerja (praktik) yang terbatas dan jumlah pasien yang banyak sehingga terjadi antrean untuk pasien yang ingin melakukan pengobatan. Dalam hal ini, orang tua selaku pemakai jasa lebih membutuhkan seorang pakar yang bisa memudahkan dalam mendiagnosa penyakit lebih dini agar dapat melakukan pencegahan lebih awal yang sekiranya membutuhkan waktu jika berkonsultasi dengan dokter ahli. [7]

## TINJAUAN PUSTAKA

### A.Sistem Pakar

Sistem pakar merupakan kecerdasan buatan di bidang ilmu komputer dan teknologi yang membuat komputer lebih efektif dan efesien sehingga bisa melakukan aktivitas kecerdasan seperti manusia pada umumnya. Kecerdasan buatan adalah salah satu perkembangan komputer dalam *software.*[1]

Sistem pakar atau *Expert System* biasa disebut juga dengan ***Knowledge Based System*** **yaitu suatu sistem aplikasi komputer yang digunakan dalam membantu pengambilan keputusan atau pemecahan permasalahan di bidang yang lebih spesifik. Sistem ini berjalan menggunakan pengetahuan dan metode analisis yang telah diartikan terlebih dahulu oleh ahli pakar yang sesuai dengan bidang keahliannya**.[2].

### B.Forward Chaining

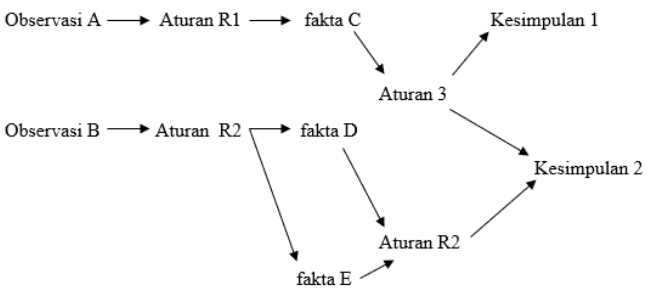
"*Forward chaining* adalah teknik pencarian yang diawali dengan fakta - fakta yang telah diketahui kemudian dicocokan dengan bagian *IF* dari rule *IF-THEN*. Bila ada fakta yang cocok dengan bagian *IF*, maka tersebut dieksekusi. Bila sebuah *rule* dieksekusi, maka sebuah fakta baru (bagian *THEN*) ditambahkan kedalam *database*.[3]

*Inferensi Forward Chaining* adalah mekanisme fungsi berfikir dan pola penalaran sistem yang digunakan oleh seorang pakar dimana di mulai dari sekumpulan data yang bersifat fakta menuju kesimpulan. Mekanisme ini akan menganalisa suatu masalah tertentu dan selanjutnya akan mencari jawaban atau kesimpulan yang terbaik dan memulai pelacakannya dengan mencocokan kaidah.[5]

### C.Balita

Balita singkatan dari bawah lima tahun adalah salah satu periode usia manusia setelah bayi sebelum anak awal. Rentang usia balita dimulai dari dua sampai dengan lima tahun, atau biasa digunakan dalam perhitungan bulan yaitu usia 24-60 bulan."[4].

## METODE




**Gambar 1.** Alur *Forward Chaining*

**Tabel 1** Data Nama Penyakit

| KODE | NAMA PENYAKIT |
|---|---|
| P01 | DBD (Demam Berdarah Dengue) |
| P02 | DD (Demam Dengue) |
| P03 | Demam Thypoid |
| P04 | Malaria |

**Tabel 1** Data Gejala

| KODE | NAMA GEJALA |
|---|---|
| G01 | Air Liur Berlebihan |
| G02 | BAB Cair (Lebih Dari 10x dalam 24 Jam) |
| G03 | Batuk |
| G04 | Batuk Berkepanjangan (Karena Debu, Asap dan Udara) |
| G05 | Batuk dan Berdahak |
| G06 | Batuk dan Berdahak (Dengan Nafas Cepat) |
| G07 | Batuk dan Berdahak (Lebih Dari 3 Minggu) |
| G08 | Bengek |
| G09 | Berat Badan Turun |
| G10 | Bercak Koplik/Koplik Spot (Bintik Putih Kecil Yang Dikelilingi Cincin Merah) |
| G11 | Berkeringat (Secara Berlebihan) |
| G12 | Berpergian Kedaerah Endemis |
| G13 | Bibir Kering dan Pahit |
| G14 | Cengeng |
| G15 | Dehidrasi |
| G16 | Demam |
| G17 | Demam (Lebih Dari 2 Minggu) |
| G18 | Demam (Lebih dari 7 hari dengan suhu turun pada pagi-siang hari dan suhu naik pada sore-malam hari) |
| G19 | Demam (Sampai Mengigil Lebih Dari 40˚C) |
| G20 | Demam (Sebelum Timbul Luka) |
| G21 | Demam (Timbul mendadak secara terus-menerus selama 2-7 hari dengan suhu 38˚C-40˚C) |
| G22 | Diare / Susah BAB (Kontipasi) |

**Tabel 3.5** Aturan Pengambilan Keputusan

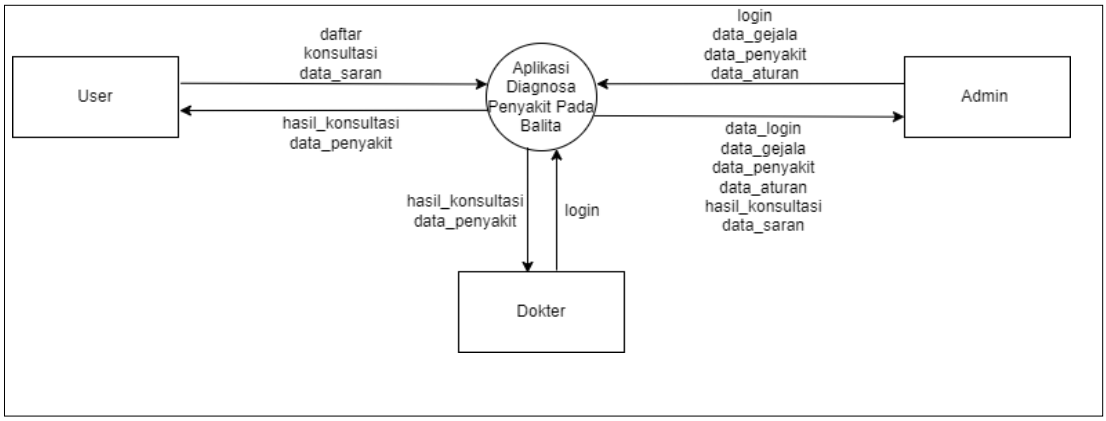
| IF | THEN | Rumus |
|---|---|---|
| G19 and G56 and G32 and G44 and G49 and G29 | P01 | $\frac{n}{6}100 = XY\%$ |
| G19 and G56 and G32 and G44 and G29 | P02 | $\frac{n}{5}100 = XY\%$ |
| G17 and G32 and G33 and G50 and G12 and G38 and G20 and G44 and G53 and G29 and G27 | P03 | $\frac{n}{11}100 = XY\%$ |
| G11 and G18 and G29 and G32 and G44 and G20 and G27 and G10 and G23 | P04 | $\frac{n}{9}100 = XY\%$ |
| G15 and G05 and G59 and G28 and G39 and G51 and G69 | P05 | $\frac{n}{7}100 = XY\%$ |
| G60 and G58 and G04 and G07 and G40 and G48 and G68 and G15 and G39 and G32 and G57 | P06 | $\frac{n}{11}100 = XY\%$ |
| G51 and G22 and G59 and G03 | P07 | $\frac{n}{4}100 = XY\%$ |

| | | |
|---|---|---|
| G25 and G15 and G36 and G26 | P08 | $\frac{n}{4}100 = XY\%$ |
| G61 and G52 and G41 and G67 and G55 | P09 | $\frac{n}{5}100 = XY\%$ |
| G30 and G16 and G06 and G08 and G50 and G32 and G59 | P10 | $\frac{n}{7}100 = XY\%$ |
| G02 and G63 and G64 and G53 and G15 and G50 and G13 and G23 and G44 and G32 and G35 and G66 and G31 | P11 | $\frac{n}{13}100 = XY\%$ |
| G15 and G70 and G54 and G37 and G09 and G42 | P12 | $\frac{n}{6}100 = XY\%$ |

## HASIL DAN PEMBAHASAN

### A. Diagram Konteks

Berikut ini adalah Diagram Konteks dari Aplikasi Sistem Pakar Diagnosa Penyakit Pada Balita Dengan Metode *Forward Chaining* Pada Klinik dan Apotek Permata Medika Berbasis *Website*.

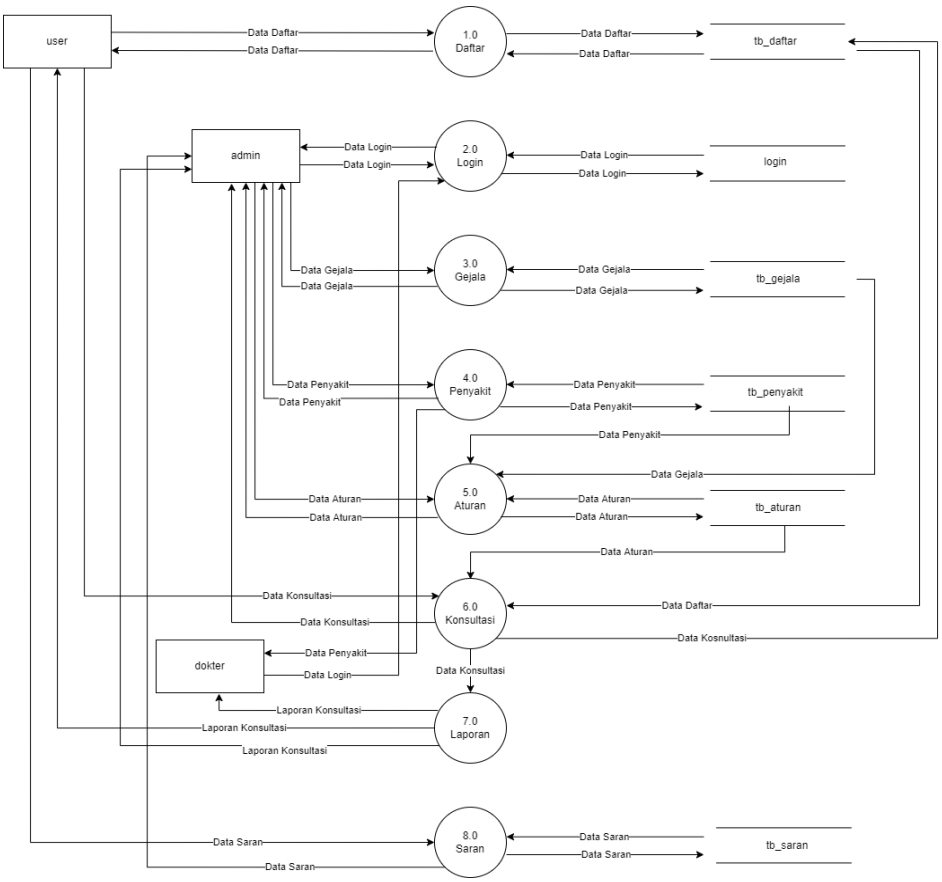



**Gambar 2.**

### B. *Data Flow Diagram* (DFD)

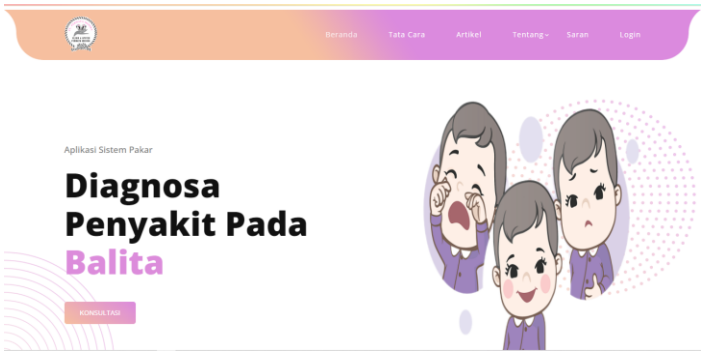
dari Aplikasi Sistem Pakar Diagnosa Penyakit Pada Balita dengan Metode *Forward Chaining* pada Klinik dan Apotek Permata Medika Berbasis *Website*.

#### 5.1.2.3.1 DFD Level 1




**Gambar 3** *Data Flow Diagram* (DFD) Level 1.

## Tampilan Halaman Awal Beranda




**Gambar 4** Tampilan halaman awal beranda

**Tampilan Halaman Awal Tata Cara**


**Gambar 5** Tampilan halaman awal tata cara

**Tampilan Halaman Awal Artikel**


**Gambar 6** Tampilan halaman awal artikel

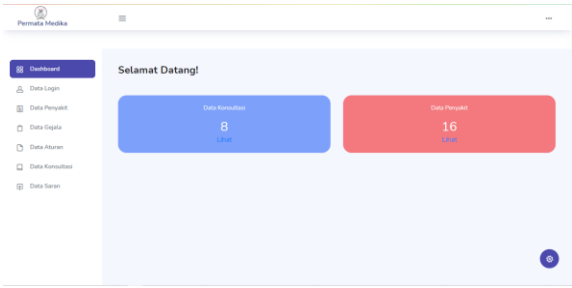
**Tampilan Halaman Awal Tentang Aplikasi**


**Gambar 7** Tampilan halaman tentang aplikasi

### 4.5.7 Tampilan Halaman *Login*

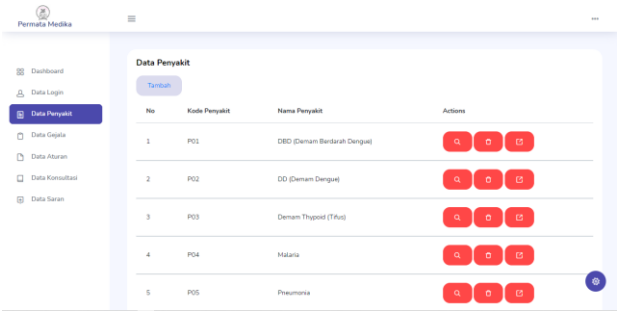

**Gambar 8** Tampilan halaman *login*

**Tampilan Halaman *Dashboard* Admin**



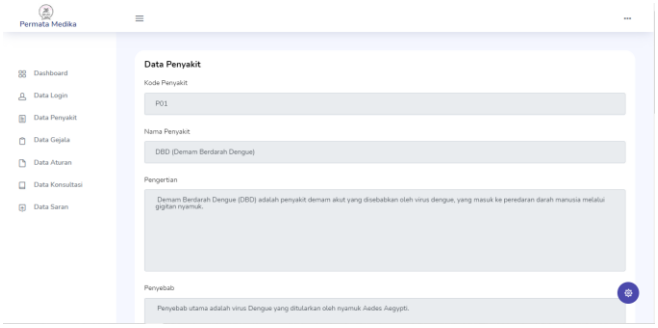

**Gambar 9** Tampilan halaman *dashboard* admin

**Tampilan Halaman Data Penyakit**




**Gambar10** Tampilan halaman data penyakit

**Tampilan Halaman Detail Data Penyakit**




**Gambar 11** Tampilan halaman detail data penyakit

## KESIMPULAN

1. Aplikasi ini mampu memberikan hasil analisa dengan metode *Forward Chaining* untuk memberikan diagnosa mengenai penyakit yang diderita balita melalui gejala-gejala yang telah ditambahkan ke sistem sesuai kondisi yang dirasakan dengan hasil *output* berupa nama penyakit dan informasi mengenai detail penyakit.
2. Aplikasi ini dapat membantu *user* dalam melakukan diagnosa penyakit yang sedang diderita balita dan juga dapat membantu pekerjaan dokter ahli dalam mendiagnosa penyakit pada balita dengan tingkat akurasi 87,5% berdasarkan pengujian yang telah dilakukan.

DAFTAR PUSTAKA

[1]. Arisandi, D., & Sari, I. P. (2021). *Sistem Pakar dengan Fuzzy Expert System*. Ponorogo: Gracias Logis Kreatif.

[2]. Ariani, F., Fahmi, M., & Taufik, A. (2019). Perancangan Sistem Informasi Perpustakaan Berbasis Website dengan Metode Framework For The Application System Thinking (FAST). *Inti Nusa Mandiri*, 21-26.

[3]. Egasari, A., Puspitaningrum, D., & Prawito, P. (2017). Sistem Pakar Identifikasi KEsesuaian Lahan untuk Tanaman Perkebunan di Provinsi Bengkulu dengan Metode Bayes dan Inferensi Forward Chaining. *Jurnal Rekursif*, 134-146.

[4]. Marmi dan Rahardjo (2018:2), "Balita singkatan dari bawah lima tahun adalah salah satu periode usia. https://scholar.google.co.id/scholar?q=related:f_jRJUD7dykJ:scholar.google.com/&scioq=Menurut+Marmi+dan+Rahardjo+(2018:2),&hl=id&as_sdt=0,5&as_vis=1 (akses tanggal 20 juli 2022)

[5]. Hayadi, B. H. (2018). *Sistem Pakar Penyelesaian Kasus Menentukan Minat Baca, Kecenderungan, dan Karakter Siswa dengan Metode Forward Chaining*. Yogyakarta: Deepublish.

[6]. Ramadhan, P. S., & Pane, U. F. (2018). *Mengenal Metode Sistem Pakar*. Ponorogo: Uwais Inspirasi Indonesia.

[7]. Swetapadma, A., & Sarraf, J. (2018). *Expert System Techinques in Biomedical Science Practice*. United State of America: IGI Global.

JREEC
JOURNAL RENEWABLE ENERGY ELECTRONICS AND CONTROL
homepage URL : https://ejurnal.itats.ac.id/jreec

# APLIKASI *EMPLOYEE SELF SERVICE* (ESS) MENGGUNAKAN METODE *ACTION RESEARCH LIFE CYCLE* BERBASIS WEBSITE PADA MASA PANDEMIK COVID19 (STUDI KASUS : PT. BANK PEMBANGUNAN DAERAH SUMATERA SELATAN DAN BANGKA BELITUNG CABANG KM 12 PALEMBANG)

**Leni Novianti[1], Henny Madora[2], Yusniarti[3], Desi Dwi S[4], Sari Dwi Safitri[5], Alan Novi Tompunu[6]**
[1-5]Program Studi Manajemen Informatika, [6] Teknik Komputer
Politeknik Negeri Srwijaya Srijaya Negara Bukit Besar Palembang

[1-4,6]Program Studi Manajemen Informatika,[5]Teknik Komputer
Politeknik Negeri Srwijaya Srijaya Negara Bukit Besar Palembang

**INFORMASI ARTIKEL**

Jurnal JREEC – Volume 03
Nomer 01, Juni 2023

Halaman:
9 – 16
Tanggal Terbit :
06 Juni 2023

DOI:
10.31284/j.JREEC.2023.v31i.4242

***ABSTRACT***

The purpose of making this Final Project is to create an Employee Self Service Application at PT Bank Pembangunan Daerah Sumatera Selatan and Bangka Belitung based on a website. The data collection method used is primary data in the form of observations and interviews, and secondary data in the form of literature, books, articles, theories, papers and other references related to the material for preparing this practical work report. This application development uses the PHP programming language, Sublime Text, Xampp and MySQL database. The system development model applied to this application is the waterfall model which provides a sequential or sequential software lifeflow approach starting from analysis, design, coding, testing and maintenance. This application contains a menu of user data, absent data, login data, salary data, and employee leave data.

Keywords: Employee Self Service, Service, Regional Development Bank.

**EMAIL**

leninovianti16@gmail.com
henny_madora_mi@polsri.ac.id
yusniarti_mi@polsri.ac.id
alan_nt@gmail.com

Jurusan Teknik Elektro-ITATS
Alamat:
Jl. Arief Rachman Hakim No.100,Surabaya 60117,
Telp/Fax: 031-5997244



**ABSTRAK**

Tujuan dari pembuatan Tugas Akhir adalah membuat sebuah Aplikasi *Employee Self Service* di PT Bank Pembangunan Daerah Sumatera Selatan dan Bangka Belitung Berbasis *Website*. Metode pengumpulan data yang digunakan adalah data primer yang berupa pengamatan (observasi) dan wawancara, dan data sekunder yang berupa *literature*, buku, artikel, teori, makalah serta referensi lainnya yang berkaitan dengan materi penyusunan laporan kerja praktek ini. Pembangunan Aplikasi ini menggunakan bahasa pemrograman *PHP*, *Sublime Text*, *Xampp* dan database *MySQL*. Model pengembangan sistem yang diterapkan pada aplikasi ini adalah model *waterfall* yang menyediakan pendekatan alur hidup perangkat lunak secara sekuensial atau terurut mulai dari analisis, deasin, pengkodean, pengujian dan pemeliharaan. Aplikasi ini berisi menu data user, data absen, data data login, data gaji, dan data cuti karyawan.

Kata kunci : *Employee Self Service*, *Service*, Bank Pembangunan Daerah.

## PENDAHULUAN

Bank Sumsel Babel saat ini memiliki 18 Kantor Cabang, 31 Kantor Cabang Pembantu, dan 23 Kantor Kas yang tersebar di seluruh daerah provinsi Sumatera Selatan dan Bangka Belitung, dan juga telah memiliki Unit Syariah. Sebagai perusahaan yang besar PT. Bank Pembangunan Daerah Sumatera Selatan dan Bangka Belitung Cabang Pembantu Km.12 Palembang memiliki akses kehadiran untuk karyawannya, terdapat sebuah sistem kehadiran yang menggunakan sidik jari didalamnya. Dalam keadaan yang sekarang sedang dihadapi, yaitu *Covid-19*. Untuk mencegah penularan wabah tersebut ada baiknya perusahaan tersebut tidak banyak menggunakan kontak fisik, seperti menggunakan sidik jari sebagai kehadiran karyawannya. Sehingga saat ini sistem kehadiran karyawan menggunakan sidik jari tidak digunakan pada saat ini. Perusahaan tersebut harus menggunakan alternatif lain dari sidik jari, seperti akses kehadiran melalui aplikasi *Employee Self Service* agar terciptanya kondisi yang aman bagi area perkantoran PT. Bank Pembangunan Daerah Sumatera Selatan dan Bangka Belitung Cabang Pembantu KM.12 Palembang.

Dengan pertimbangan diatas pihak PT. Bank Pembangunan Daerah Sumatera Selatan dan Bangka Belitung mengusung suatu sistem absensi dan *Human Resource* berupa Aplikasi *Employee Self Service*. Teknologi ini mampu membantu dalam memaksimalkan keefektifan absensi dan kegiatan *Human Resource* di area perkantoran PT. Bank Pembangunan Daerah Sumatera Selatan dan Bangka Belitung Cabang Pembantu KM.12 Palembang, sistem ini terkoneksi melalui sebuah jaringan yang terbentuk di area perkantoran PT. Bank Pembangunan Daerah Sumatera Selatan dan Bangka Belitung Cabang Pembantu Km.12 Palembang, sistem ini menggunakan konektivitas *wifi* atau paket data *handphone* ini sehingga dapat diakses dimanapun selagi masih ada jaringan internet.

## TINJAUAN PUSTAKA

### A.Sistem Pakar

Sistem pakar merupakan kecerdasan buatan di bidang ilmu komputer dan teknologi yang membuat komputer lebih efektif dan efesien sehingga bisa melakukan aktivitas kecerdasan seperti manusia pada umumnya. Kecerdasan buatan adalah salah satu perkembangan komputer dalam *software.*[1]

Sistem pakar atau *Expert System* biasa disebut juga dengan ***Knowledge Based System*** **yaitu suatu sistem aplikasi komputer yang digunakan dalam membantu pengambilan keputusan atau pemecahan permasalahan di bidang yang lebih spesifik. Sistem ini berjalan menggunakan pengetahuan dan metode analisis yang telah diartikan terlebih dahulu oleh ahli pakar yang sesuai dengan bidang keahliannya**.[2].

### B.Forward Chaining

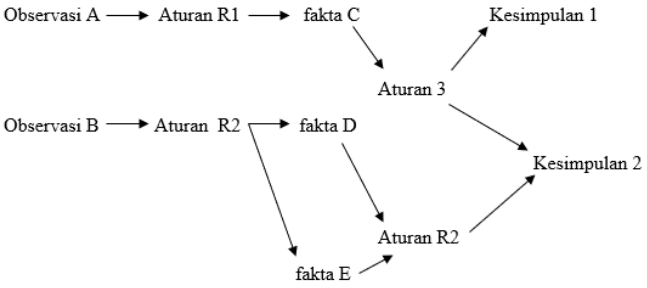
"*Forward chaining* adalah teknik pencarian yang diawali dengan fakta - fakta yang telah diketahui kemudian dicocokan dengan bagian *IF* dari rule *IF-THEN*. Bila ada fakta yang cocok dengan bagian *IF*, maka tersebut dieksekusi. Bila sebuah *rule* dieksekusi, maka sebuah fakta baru (bagian *THEN*) ditambahkan kedalam *database*.[3]

*Inferensi Forward Chaining* adalah mekanisme fungsi berfikir dan pola penalaran sistem yang digunakan oleh seorang pakar dimana di mulai dari sekumpulan data yang bersifat fakta menuju kesimpulan. Mekanisme ini akan menganalisa suatu masalah tertentu dan selanjutnya akan mencari jawaban atau kesimpulan yang terbaik dan memulai pelacakannya dengan mencocokan kaidah.[5]

### C.Balita

Balita singkatan dari bawah lima tahun adalah salah satu periode usia manusia setelah bayi sebelum anak awal. Rentang usia balita dimulai dari dua sampai dengan lima tahun, atau biasa digunakan dalam perhitungan bulan yaitu usia 24-60 bulan."[4].

**METODE**




**Gambar 1.** Alur *Forward Chaining*

**Tabel 1** Data Nama Penyakit

| KODE | NAMA PENYAKIT |
|---|---|
| P01 | DBD (Demam Berdarah Dengue) |
| P02 | DD (Demam Dengue) |
| P03 | Demam Thypoid |
| P04 | Malaria |

**Tabel 1** Data Gejala

| KODE | NAMA GEJALA |
|---|---|
| G01 | Air Liur Berlebihan |
| G02 | BAB Cair (Lebih Dari 10x dalam 24 Jam) |
| G03 | Batuk |
| G04 | Batuk Berkepanjangan (Karena Debu, Asap dan Udara) |
| G05 | Batuk dan Berdahak |
| G06 | Batuk dan Berdahak (Dengan Nafas Cepat) |
| G07 | Batuk dan Berdahak (Lebih Dari 3 Minggu) |
| G08 | Bengek |
| G09 | Berat Badan Turun |
| G10 | Bercak Koplik/Koplik Spot (Bintik Putih Kecil Yang Dikelilingi Cincin Merah) |
| G11 | Berkeringat (Secara Berlebihan) |
| G12 | Berpergian Kedaerah Endemis |
| G13 | Bibir Kering dan Pahit |
| G14 | Cengeng |
| G15 | Dehidrasi |
| G16 | Demam |
| G17 | Demam (Lebih Dari 2 Minggu) |
| G18 | Demam (Lebih dari 7 hari dengan suhu turun pada pagi-siang hari dan suhu naik pada sore-malam hari) |
| G19 | Demam (Sampai Mengigil Lebih Dari 40˚C) |
| G20 | Demam (Sebelum Timbul Luka) |

| | |
|---|---|
| G21 | Demam (Timbul mendadak secara terus-menerus selama 2-7 hari dengan suhu 38˚C-40˚C) |
| G22 | Diare / Susah BAB (Kontipasi) |

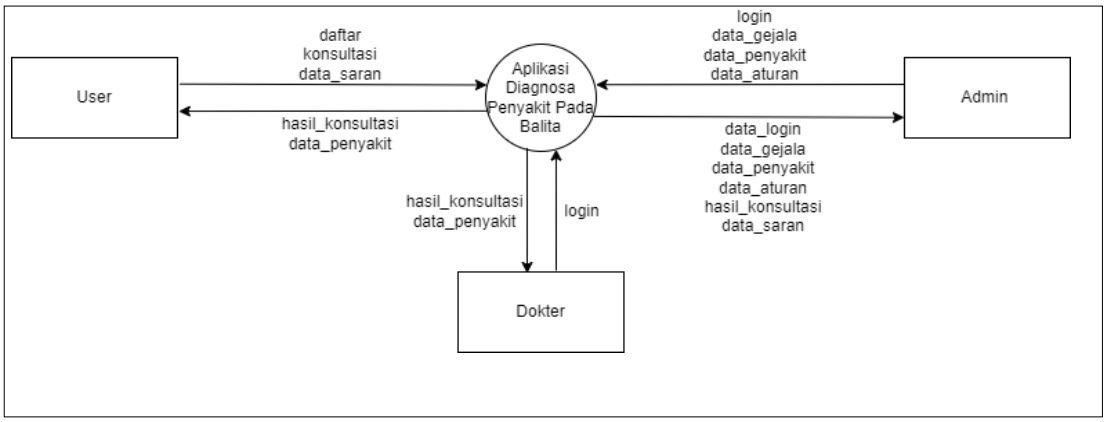
**Tabel 3.5** Aturan Pengambilan Keputusan

| IF | THEN | Rumus |
|---|---|---|
| G19 and G56 and G32 and G44 and G49 and G29 | P01 | $\frac{n}{6}100 = XY\%$ |
| G19 and G56 and G32 and G44 and G29 | P02 | $\frac{n}{5}100 = XY\%$ |
| G17 and G32 and G33 and G50 and G12 and G38 and G20 and G44 and G53 and G29 and G27 | P03 | $\frac{n}{11}100 = XY\%$ |
| G11 and G18 and G29 and G32 and G44 and G20 and G27 and G10 and G23 | P04 | $\frac{n}{9}100 = XY\%$ |
| G15 and G05 and G59 and G28 and G39 and G51 and G69 | P05 | $\frac{n}{7}100 = XY\%$ |
| G60 and G58 and G04 and G07 and G40 and G48 and G68 and G15 and G39 and G32 and G57 | P06 | $\frac{n}{11}100 = XY\%$ |
| G51 and G22 and G59 and G03 | P07 | $\frac{n}{4}100 = XY\%$ |
| G25 and G15 and G36 and G26 | P08 | $\frac{n}{4}100 = XY\%$ |
| G61 and G52 and G41 and G67 and G55 | P09 | $\frac{n}{5}100 = XY\%$ |
| G30 and G16 and G06 and G08 and G50 and G32 and G59 | P10 | $\frac{n}{7}100 = XY\%$ |
| G02 and G63 and G64 and G53 and G15 and G50 and G13 and G23 and G44 and G32 and G35 and G66 and G31 | P11 | $\frac{n}{13}100 = XY\%$ |
| G15 and G70 and G54 and G37 and G09 and G42 | P12 | $\frac{n}{6}100 = XY\%$ |

## HASIL DAN PEMBAHASAN

### A. Diagram Konteks

Berikut ini adalah Diagram Konteks dari Aplikasi Sistem Pakar Diagnosa Penyakit Pada Balita Dengan Metode *Forward Chaining* Pada Klinik dan Apotek Permata Medika Berbasis *Website*.

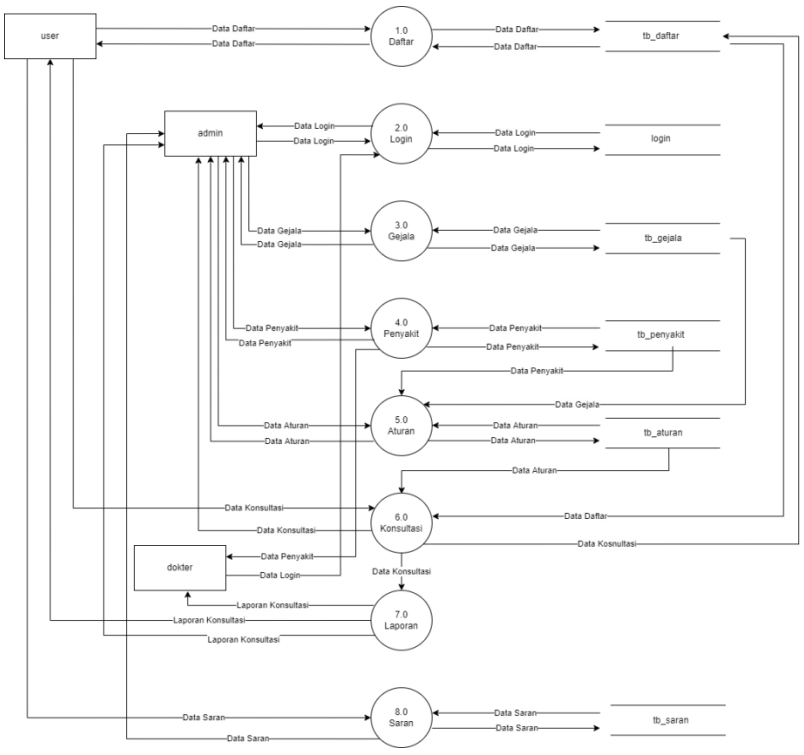



**Gambar 2.**

**B. *Data Flow Diagram* (DFD)**

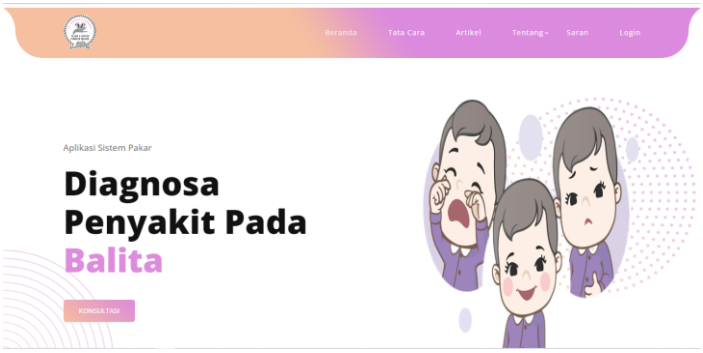
dari Aplikasi Sistem Pakar Diagnosa Penyakit Pada Balita dengan Metode *Forward Chaining* pada Klinik dan Apotek Permata Medika Berbasis *Website*.

**5.1.2.3.1 DFD Level 1**




**Gambar 3** *Data Flow Diagram* (DFD) Level 1.

**Tampilan Halaman Awal Beranda**




**Gambar 4** Tampilan halaman awal beranda

**Tampilan Halaman Awal Tata Cara**


**Gambar 5** Tampilan halaman awal tata cara

**Tampilan Halaman Awal Artikel**


**Gambar 6** Tampilan halaman awal artikel

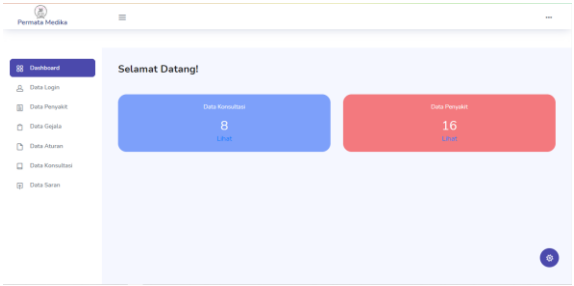
**Tampilan Halaman Awal Tentang Aplikasi**


**Gambar 7** Tampilan halaman tentang aplikasi

**Tampilan Halaman *Login***

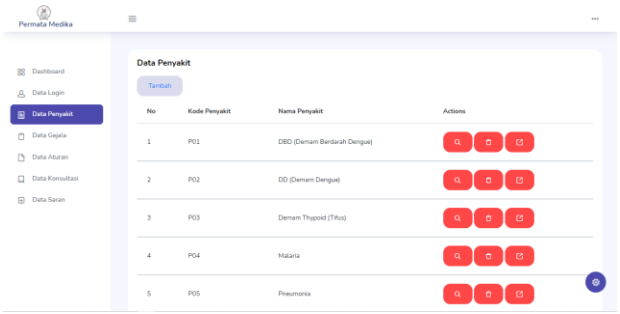

**Gambar 8** Tampilan halaman *login*

**Tampilan Halaman *Dashboard* Admin**



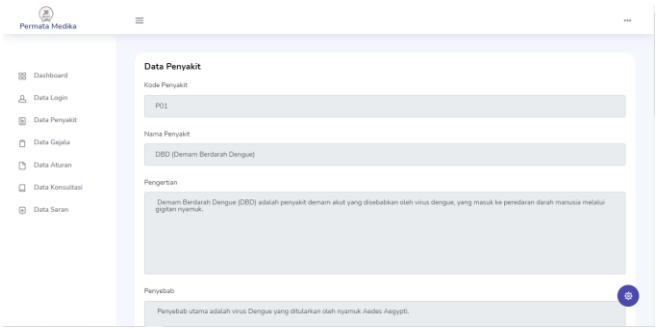

**Gambar 9** Tampilan halaman *dashboard* admin

**Tampilan Halaman Data Penyakit**




**Gambar10** Tampilan halaman data penyakit

**Tampilan Halaman Detail Data Penyakit**




**Gambar 11** Tampilan halaman detail data penyakit

## KESIMPULAN

1. Aplikasi ini mampu memberikan hasil analisa dengan metode *Forward Chaining* untuk memberikan diagnosa mengenai penyakit yang diderita balita melalui gejala-gejala yang telah ditambahkan ke sistem sesuai kondisi yang dirasakan dengan hasil *output* berupa nama penyakit dan informasi mengenai detail penyakit.
2. Aplikasi ini dapat membantu *user* dalam melakukan diagnosa penyakit yang sedang diderita balita dan juga dapat membantu pekerjaan dokter ahli dalam mendiagnosa penyakit pada balita dengan tingkat akurasi 87,5% berdasarkan pengujian yang telah dilakukan.

DAFTAR PUSTAKA

[1]. Arisandi, D., & Sari, I. P. (2021). *Sistem Pakar dengan Fuzzy Expert System.* Ponorogo: Gracias Logis Kreatif.

[2]. Ariani, F., Fahmi, M., & Taufik, A. (2019). Perancangan Sistem Informasi Perpustakaan Berbasis Website dengan Metode Framework For The Application System Thinking (FAST). *Inti Nusa Mandiri*, 21-26.

[3]. Egasari, A., Puspitaningrum, D., & Prawito, P. (2017). Sistem Pakar Identifikasi KEsesuaian Lahan untuk Tanaman Perkebunan di Provinsi Bengkulu dengan Metode Bayes dan Inferensi Forward Chaining. *Jurnal Rekursif*, 134-146.

[4]. Marmi dan Rahardjo (2018:2), “Balita singkatan dari bawah lima tahun adalah salah satu periode usia. https://scholar.google.co.id/scholar?q=related:f_jRJUD7dykJ:scholar.google.com/&scioq=Menurut+Marmi+dan+Rahardjo+(2018:2),&hl=id&as_sdt=0,5&as_vis=1 (akses tanggal 20 juli 2022)

[5]. Hayadi, B. H. (2018). *Sistem Pakar Penyelesaian Kasus Menentukan Minat Baca, Kecenderungan, dan Karakter Siswa dengan Metode Forward Chaining.* Yogyakarta: Deepublish.

[6]. Ramadhan, P. S., & Pane, U. F. (2018). *Mengenal Metode Sistem Pakar.* Ponorogo: Uwais Inspirasi Indonesia.

[7]. Swetapadma, A., & Sarraf, J. (2018). *Expert System Techinques in Biomedical Science Practice.* United State of America: IGI Global.

JREEC
JOURNAL RENEWABLE ENERGY ELECTRONICS AND CONTROL
homepage URL : https://ejurnal.itats.ac.id/jreec

# SISTEM PAKAR UNTUK MENDIAGNOSA PENYAKIT *COMPUTER VISION SYNDROME* (CVS)".

**M.Noval[1], Leni Novianti[2], Denny Alfian[3], Tri Seltawika[4], Alan Novi Tompunu[5]**
[1-4]Program Studi Manajemen Informatika, [5] Teknik Komputer
Politeknik Negeri Srwijaya Srijaya Negara Bukit Besar Palembang

[1-4]Program Studi Manajemen Informatika,[5]Teknik Komputer
Politeknik Negeri Srwijaya Srijaya Negara Bukit Besar Palembang

**INFORMASI ARTIKEL**

Jurnal JREEC – Volume 03
Nomer 01, Juni 2023

Halaman:
17 – 26
Tanggal Terbit :
06 Juni 2023

DOI:
10.31284/j.JREEC.2023.v31i.4247

***ABSTRACT***

This study aims to provide comparative information to determine which method is more accurate, effective and efficient in diagnosing CVS from the symptoms described by an ophthalmologist or CVS. The methods used for comparison are the Forward Chaining Inference method and the Naive Bayes method, so that the final result of the comparison of these two methods is expected to be able to get the right solution for the symptoms of people with CVS disease. System design using the Unified Modeling Language (UML). The tools used to build are xampp (App Server), Visual Studio Code, the programming language used is php and the CodeIgniter framework. The application designed in this study is expected to facilitate the process of diagnosing computer vision syndrome (CVS).

Keywords: *computer vision syndrome* (CVS), *Inferensi Forward Chaining* and *Naive Bayes Method*, *Unified Modeling Language* (UML)..

**EMAIL**

m_noval_mi@polsri.ac.id
leninovianti16@gmail.com
denny_alfian_mi@polsri.ac.id
triselta05@gmail.com
alan_nt@gmail.com

Jurusan Teknik Elektro-ITATS
Alamat:
Jl. Arief Rachman Hakim No.100,Surabaya 60117,
Telp/Fax: 031-5997244



**ABSTRAK**

Dalam penelitian ini bertujuan untuk memberikan informasi perbandingan untuk menentukan metode mana yang lebih akurat, efektif, dan efesien dalam mendiagnosa penyakit CVS dari gejala-gejala yang dijelaskan oleh ahli pakar penyakit mata atau CVS. Metode yang menjadi perbandingan adalah metode *Inferensi Forward Chaining* dan metode *Naive Bayes*, sehingga hasil akhir dari perbandingan kedua metode ini diharapkan dapat mendapatkan solusi yang tepat dari gejala penderita penyakit CVS. Perancangan sistem dengan menggunakan *Unified Modeling Language* (UML). *Tools* yang digunakan untuk membangun adalah *xampp (App Server), Visual Studio Code*, bahasa pemrograman yang digunakan adalah php dan *framework Codeigniter*. Aplikasi yang dirancang dalam penelitian ini diharapkan dapat mempermudah proses diagnosa penyakit *computer vision syndrome* (CVS).

Kata kunci : *computer vision syndrome* (CVS), *Inferensi Forward Chaining* dan metode *Naive Bayes*, *Unified Modeling Language* (UML).

## PENDAHULUAN

Menurut Data & Statistik Kementerian Komunikasi dan Informatika RI, pada tahun 2019 persentase kepemilikan handphone ada sebanyak 73,7% sedangkan kepemilikan komputer sebanyak 25,2%. Sedangkan menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mengungkapkan jumlah pengguna internet di Indonesia mencapai 196.71 juta orang hingga akhir tahun 2019. Banyak penelitian khususnya di negara maju menunjukkan adanya hubungan antara penggunaan perangkat-perangkat tersebut dengan kesehatan mata yang menimbulkan berbagai gejala.

Kelompok gejala yang di klasifikasikan sebagai CVS termasuk ketegangan mata, sakit kepala, pandangan kabur, nyeri pada leher dan pundak, dan mata kering .Melihat layar digital menunjukkan perbedaan dengan membaca sesuatu yang dicetak karena huruf cetak pada koran atau buku umumnya memiliki karakter hitam padat dengan batas yang jelas dan secara signifikan lebih kontras dan tidak menimbulkan masalah bagi mata yang sehat. Namun pada layar monitor tidak memiliki kontras, selain itu adanya silau dan pantulan cahaya layar monitor menyebabkan kesulitan dalam melihat. Jadi, untuk berfokus pada sesuatu dan mempertahankan fokus sangatlah sulit. Kesulitan ini menyebabkan adanya gejala pada mata .

Beberapa faktor risiko yang telah dijelaskan kemungkinan hal tersebut memiliki hubungan dengan kejadian CVS, karena penggunaan komputer merupakan sebuah kewajiban untuk memenuhi tuntutan profesi. Hal ini membuat penulis tertarik untuk membuat sistem pakar untuk diagnosa penyakit *Computer Vision Syndrome* (CVS) pada pasien Rumah Sakit Umum Pusat Dr. Mohammad Hoesin Palembang (RSUP Dr. Mohammad Hoesin Palembang).

Tujuan melakukan perbandingan ini ialah untuk menentukan metode mana yang lebih akurat, efektif, dan efesien dalam mendiagnosa penyakit CVS dari gejala-gejala yang dijelaskan oleh ahli pakar penyakit mata atau CVS. Metode yang menjadi perbandingan pada tugas akhir adalah metode *Inferensi Forward Chaining* dan metode *Naive Bayes*, sehingga hasil akhir dari perbandingan kedua metode ini diharapkan dapat mendapatkan solusi yang tepat dari gejala penderita penyakit CVS.

Data penelitian yang digunakan adalah 12 gejala dan 100 data mahasiswa dimana sebagai pengguna layar digital. Penelitian dengan uji *chi square* dilakukan untuk membandingkan penderita CVS berdasarkan jenis kelamin dengan jumlah responden yang lebih banyak, yaitu sekitar 715 responden (89,9%) pada mahasiswa pengguna layar digital. Prevalensi CVS relatif lebih banyak ditemukan pada perempuan dibandingkan pada laki-laki seperti pada hasil penelitian ini didapatkan sebanyak 70,37% responden perempuan mengalami CVS (Valetina et.al, 2016). Persentase ketepatan dalam proses pengklasifikasian terhadap aplikasi sistem pakar sebesar 83,3% berdasarkan 12 data *testing* yang diuji menunjukkan aplikasi ini cukup efektif dalam mendiagnosa penyakit (Kusbianto dkk, 2017). Penggunaan metode klasifikasi *Naive Bayes* terhadap *dataset* yang telah diambil pada objek penelitian diperoleh tingkat akurasi sebesar 73% dan termasuk kategori *Good* (Haditsah Annur, 2018).

## TINJAUAN PUSTAKA

### A. *Computer Vision Syndrome* (CVS)

Menurut (Dotulong et.al, 2021) dalam penelitian berjudul "*Computer Vision Syndrome*" menyatakan bahwa Sindom Penglihatan Komputer atau dalam bahasa inggris *Computer Vision Syndrome* merupakan sekumpulan dari keluhan pada mata yang diakibatkan oleh penggunaan layar digital terkhusus komputer dalam jangka waktu yang lama yang menyebabkan mata lelah, nyeri kepala dan gejala bervariasi lainnya dalam penelitian.[1]

Menurut Forster dalam (Baskaran, dkk , 2020), *Computer Vision Syndrome* (CVS) adalah sindrom atau penyakit dari salah satu dampak dari menghabiskan lebih banyak waktu dengan layar digital yang mengakibatkan peningkatan ketegangan mata dan masalah penglihatan.

(Sulianta, 2018), *Computer Vision Syndrome* (CVS) adalah permasalahan pada mata akibat kelelahan dan ketegangan yang disebabkan karena penggunaan komputer dalam jangka waktu lama sehingga mata terus dipaksa menatap layar monitor. Gejala-gejala yang diderita sindrom ini antara lain mata terasa kering dan gatal, mata menjadi merah dan berair, kehilangan fokus, sakit kepala, nyeri pundak, bahkan otot mata menjadi kejang.

Dari pernyataan di atas maka penulis menarik kesimpulan bahwa *Computer Vision Syndrome* merupakan sindrom akibat kelelahan dan ketegangan pada bagian mata yang disebabkan karena penggunaan komputer atau layar digital lainnya dalam jangka waktu lama.

**B. *Forward Chaining***

(Ramadhan & Pane, 2018) "*Forward chaining* adalah teknik pencarian yang diawali dengan fakta - fakta yang telah diketahui kemudian dicocokan dengan bagian *IF* dari rule *IF-THEN*. Bila ada fakta yang cocok dengan bagian *IF*, maka tersebut dieksekusi. Bila sebuah *rule* dieksekusi, maka sebuah fakta baru (bagian *THEN*) ditambahkan kedalam *database*.

(Hayadi, 2018), *Inferensi Forward Chaining* adalah mekanisme fungsi berfikir dan pola penalaran sistem yang digunakan oleh seorang pakar dimana di mulai dari sekumpulan data yang bersifat fakta menuju kesimpulan. Mekanisme ini akan menganalisa suatu masalah tertentu dan selanjutnya akan mencari jawaban atau kesimpulan yang terbaik dan memulai pelacakannya dengan mencocokan kaidah.

Menurut pendapat (Egasari, dkk , 2017) berdasarkan penelitian yang berjudul "Sistem Pakar Identifikasi Kesesuaian Lahan untuk Tanaman Perkebunan di Provinsi Bengkulu dengan Metode *Baye*s dan *Inferensi Forward Chaining*" pengertian dari *Inferensi Forward Chaining* adalah suatu pengambilan keputusan yang paling sering digunakan dalam sistem pakar dengan menggunakan proses pencarian pernyataan kesimpulan akhir dari data gejala yang disediakan.

Dari pernyataan di atas maka penulis menarik kesimpulan bahwa *Inferensi Forward Chaining* merupakan metode sistem pakar yang mencari solusi melalui masalah yang mempetimbangkan melalui fakta yang ada dan menarik kesimpulan.

**C. *Naive Bayes***

(Fadila, Rahayu, & Saputra, 2020), "*Naive Bayes* adalah pengklasifikasi jaringan Bayesian paling sederhana. Dalam *Naive Bayes*, setiap node fitur memiliki simpul kelas sebagai induknya, tetapi tidak memiliki orangtua dari node fitur lainnya. Namun pengelompokan *naive bayes* dapat bersaing dengan pengklasifikasi canggih seperti C4.5 dan masih merupakan salah satu dari 10 algoritma penambangan data teratas di dunia karena masih banyak menggunakannya".

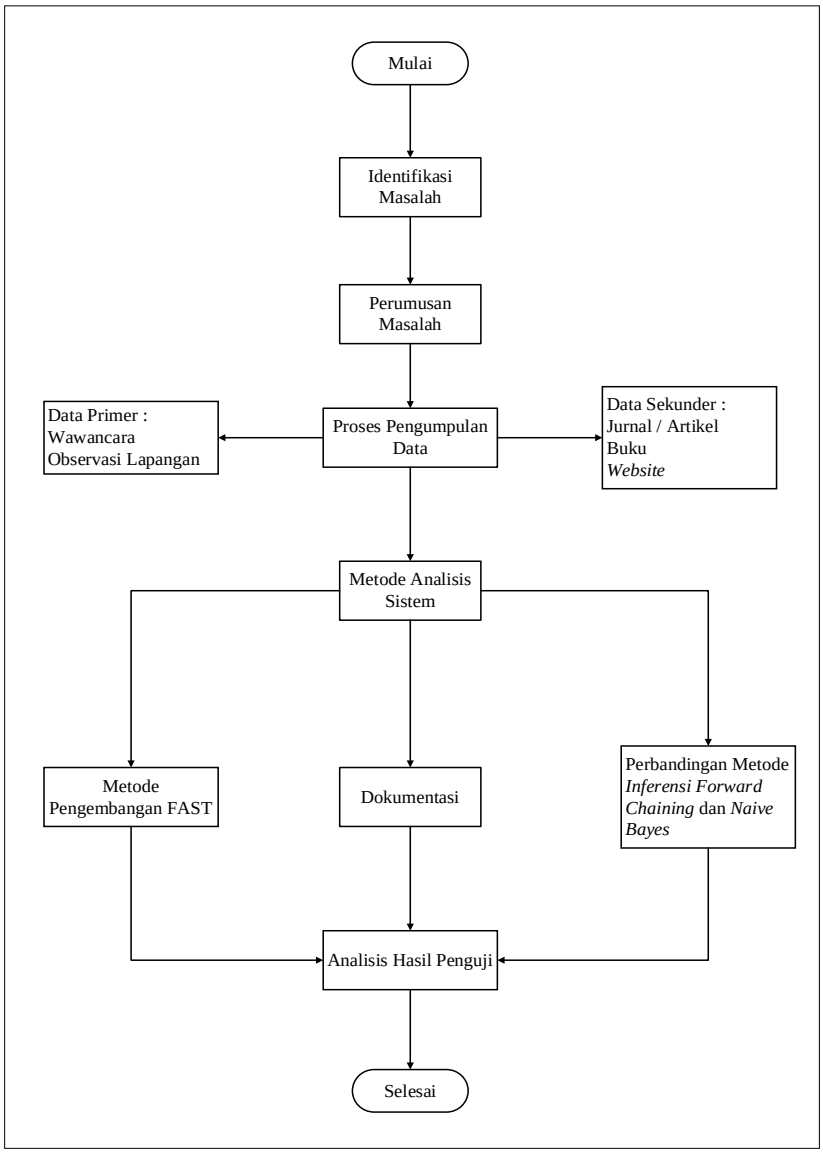
(Sidiq, Fatimah, & Riza, 2020), *Naive Bayes Classifier* merupakan sebuah pengklasifikasian probabilistik yang sederhana untuk memperkirakan sekumpulan kemungkinan dengan menampilkan jumlah frekuensi dan kombinasi dari *dataset* yang telah ada. Definisi lain mengatakan bahwa apabila diberikan nilai *output*, probabilitas mengamati secara bersama adalah produk dari probabilitas individu.

## METODE

### A. Metode Pengumpulan Data dan Kebutuhan

Studi Literatur, **m**etode ini dilakukan dengan mengkaji beberapa literatur yang berkaitan dengan penelitian pengembangan perangkat lunak berorientasi aspek, pemrograman berorientasi aspek.

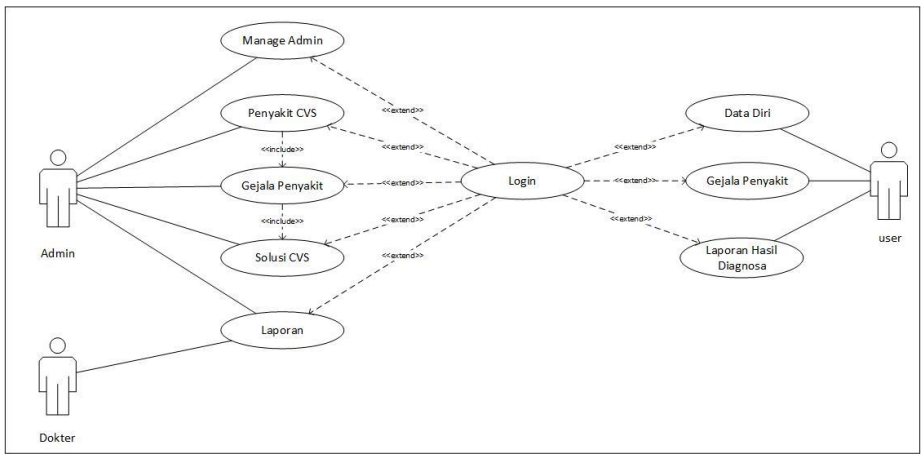
a. Buku-buku dan jurnal-jurnal penelitian yang berhubungan dengan studi kasus yang teliti.
b. Data Pasien Untuk Penyakit ***COMPUTER VISION SYNDROME*** **(CVS)**
c. Informasi dari media masa, seperti surat kabar dan internet.



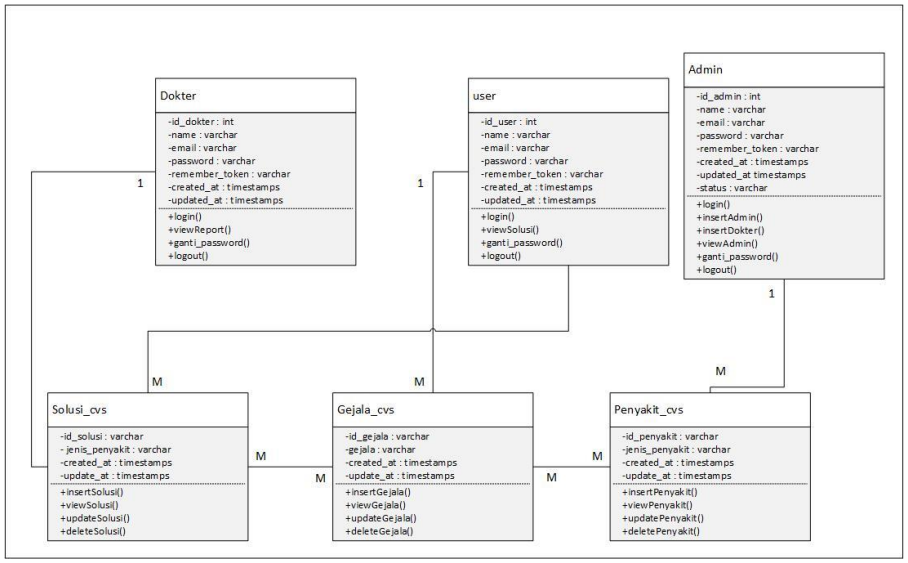

**Gambar 1.** Alur Penelitian

## HASIL DAN PEMBAHASAN

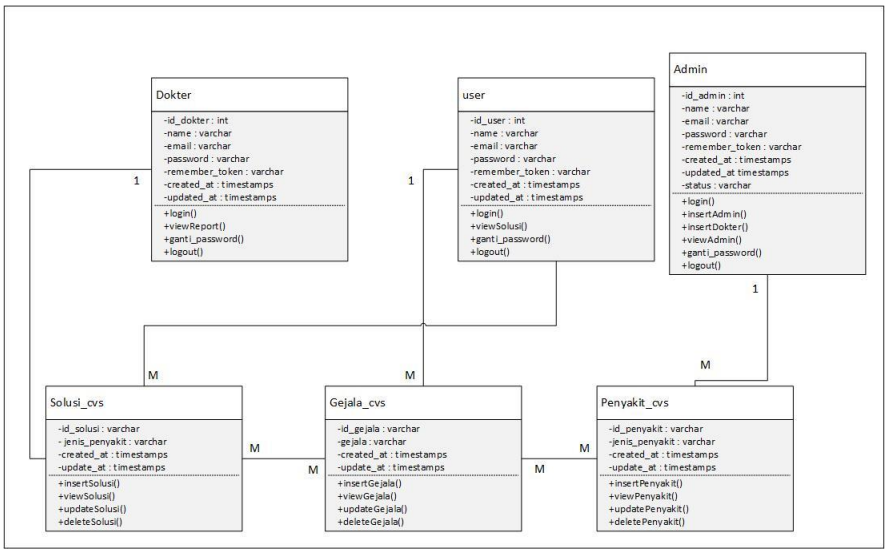
### Perancangan Sistem pada Metode Inferensi Forward Chaining




**Gambar 2** Diagram *Use Case*



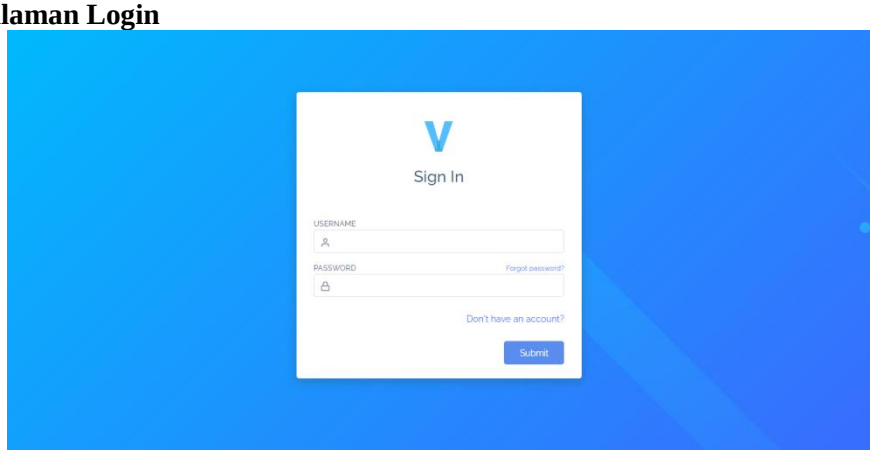

**Gambar 3** ***Diagram Class Metode Forward Chaining***




**Gambar 4** ***Diagram Class Metode Naïve bayes***

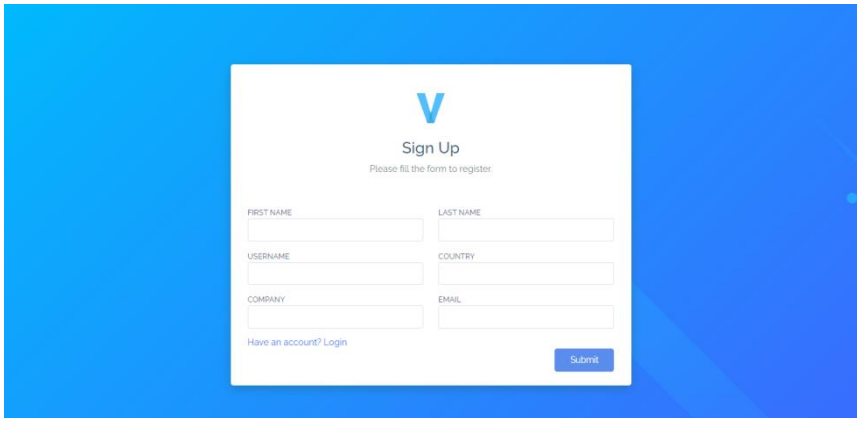
**Hasil Tampilan Aplikasi**

**Tampilan Halaman Login**



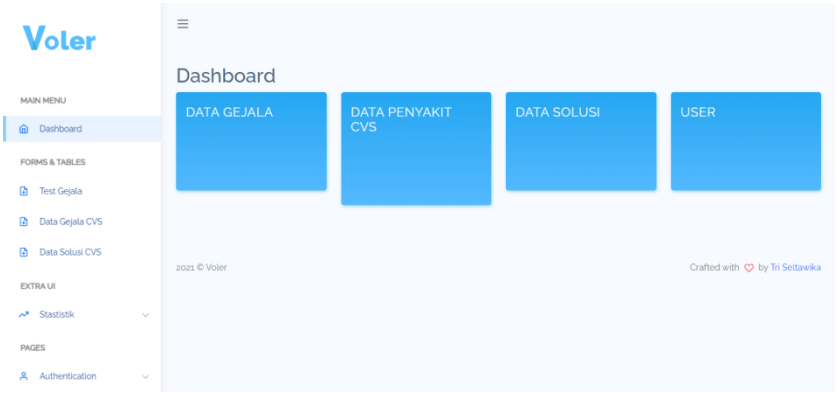

**Gambar 5** Tampilan Halaman Login

**Tampilan Halaman Registrasi Login**



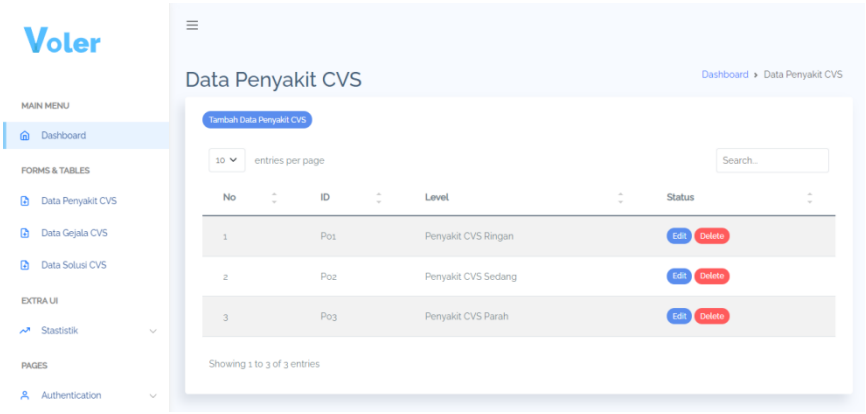

**Gambar 6** Halaman registrasi

**Tampilan Halaman Admin dan Dokter Dashboard**



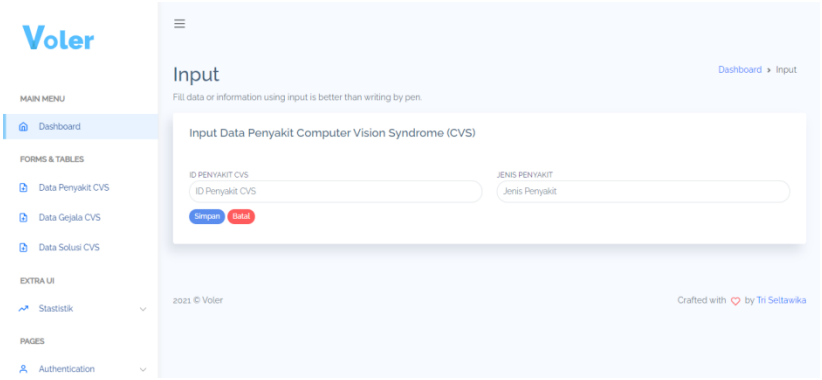

**Gambar 7** Tampilan Halaman Dashboard Admin

**Tampilan Halaman Admin Data Penyakit CVS**



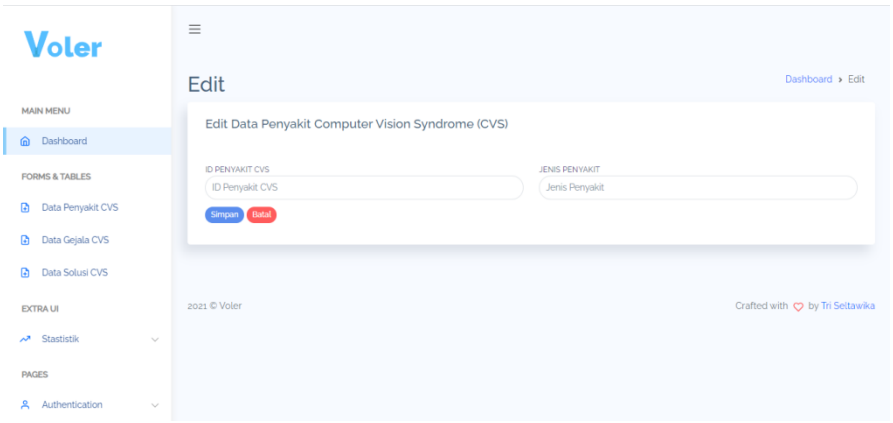

**Gambar 8** Tampilan Halaman Data Gejala Penyakit

**Tampilan Halaman Admin Input Data Penyakit**




**Gambar 9** Tampilan Halaman Input Data Penyakit

**Tampilan Halaman Admin Edit Data Penyakit CVS**

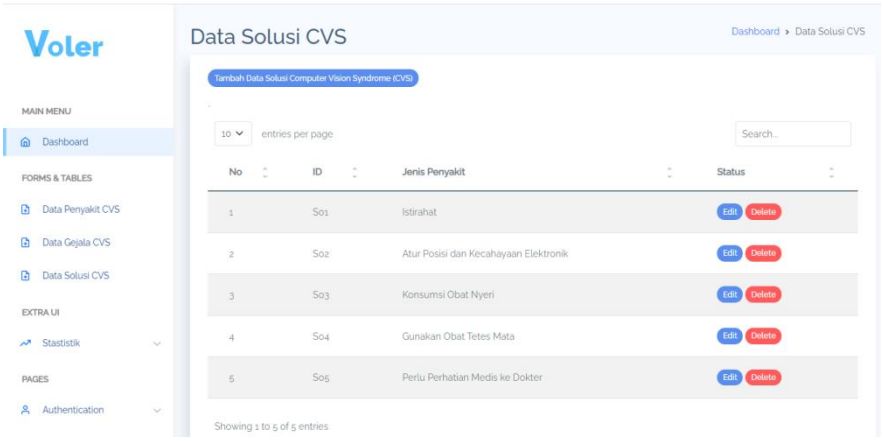



**Gambar 10** Tampilan Halaman Edit Admin Karyawan

**Tampilan Halaman Admin Data Gejala CVS**

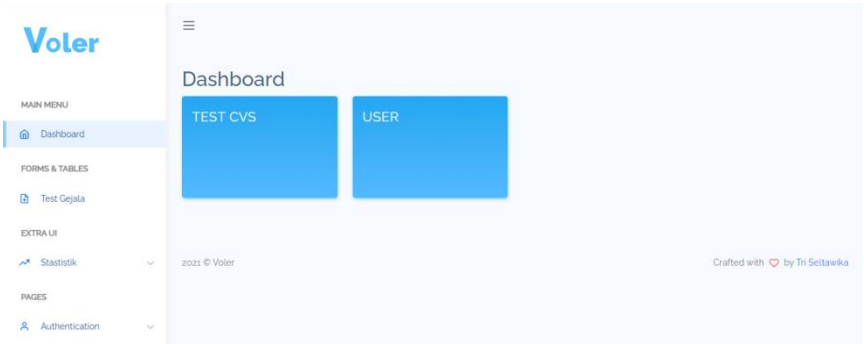

**Gambar 11** Tampilan Halaman Data Gejala CVS

**Tampilan Halaman Admin Solusi CVS**



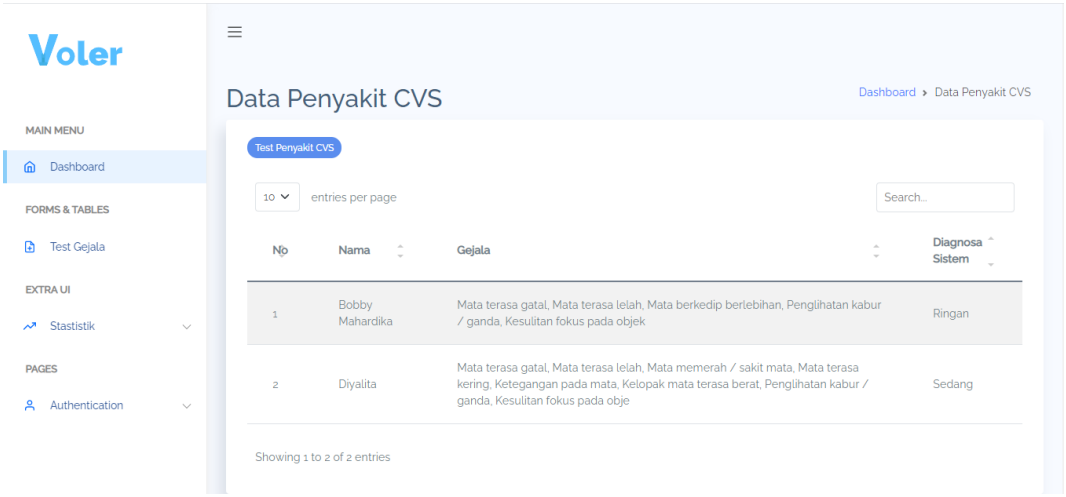

**Gambar 12** Tampilan Halaman Admin Solusi CVS

**Tampilan Halaman Utama User**




**Gambar 13** Tampilan Halaman utama user

**Tampilan Halaman Tabel Test Gejala**




**Gambar 14** Tampilan Tabel Test Gejala

**Tampilan Halaman Cetak Laporan**


**Gambar 14** Tampilan Halaman Cetak Laporan

## KESIMPULAN

1. Penelitian ini dilakukan dengan membandingkan 2 (dua) metode yaitu metode Inferensi Forward Chaining dan metode Naive Bayes yang menjadi perbandingan pada sistem ini yaitu tingkat akurasi data hasil diagnosa sistem dan dokter. Hasil perbandingan metode pada penelitian ini bahwa metode *Inferensi Forward Chaining lebih* akurat untuk mendiagnosa penyakit CVS dengan tingkat persentase 73,3% sedangkan metode *Naive Bayes* dengan tingkat persentase 50%.
2. Sistem ini juga menghasilkan *output* laporan data user yang telah mendapatkan hasil diagnosa penyakit dapat dilihat oleh Admin dan dokter berupa data statistik dan pdf. Sedangkan user memperoleh hasil laporan diagnosa penyakit yang diinputkan ke dalam sistem berupa pdf saja.

## DAFTAR PUSTAKA

[1]. Arisandi, D., & Sari, I. P. (2021). *Sistem Pakar dengan Fuzzy Expert System.* Ponorogo: Gracias Logis Kreatif.

[2]. Dotulong, D. J., Rares, L. M., & Najoan, I. H. (2021). Computer Vision Syndrome. *e-CliniC, Volume 9 Nomor 1*, 20-25.

[3]. Egasari, A., Puspitaningrum, D., & Prawito, P. (2017). Sistem Pakar Identifikasi KEsesuaian Lahan untuk Tanaman Perkebunan di Provinsi Bengkulu dengan Metode Bayes dan Inferensi Forward Chaining. *Jurnal Rekursif*, 134-146.

[4]. Fadila, Rahayu, W. I., & Saputra, M. H. (2020). *Penerapan Metode Naive Bayes dan Skala Likert pada Aplikasi Prediksi Keluylusan Mahasiswa.* Bandung: Kreatif Industri Nusantara.

[5]. Hayadi, B. H. (2018). *Sistem Pakar Penyelesaian Kasus Menentukan Minat Baca, Kecenderungan, dan Karakter Siswa dengan Metode Forward Chaining.* Yogyakarta: Deepublish.

[6]. Mudjahid, A., Darussalam, U., & Benrahman. (2020). Sistem Pakar Berbasis Web untuk Mendiagnosis Penyakit Mata Manusia menggunakan Metode NAive Bayes. *Jurnal Teknik Informatika CIT*, 16-25.

[7]. Ramadhan, P. S., & Pane, U. F. (2018). *Mengenal Metode Sistem Pakar.* Ponorogo: Uwais Inspirasi Indonesia.

[8]. Swetapadma, A., & Sarraf, J. (2018). *Expert System Techinques in Biomedical Science Practice.* United State of America: IGI Global.

JREEC
JOURNAL RENEWABLE ENERGY ELECTRONICS AND CONTROL
homepage URL : https://ejurnal.itats.ac.id/jreec

# Rancang Bangun Pengisian Otomatis Air Minum Isi Ulang dengan Sistem Full Bridge Load Cell Menggunakan Metode Filter Kalman

*Abdul Harits Mahdami[1], Wildan Agung Pambudi[2]*

*[1,2]Jurusan Teknik Elektro, Fakultas Teknik Elektro dan Teknologi Informasi, Institut Teknologi Adhi Tama Surabaya*

**INFORMASI ARTIKEL**

Jurnal JREEC – Volume 03 Nomer 01, Juni 2023

Halaman:
43-47
Tanggal Terbit :
06 Juni 2023

DOI:
10.31284/j.JREEC.2023.V31i.4476

***ABSTRACT***

*A Load Cell is a detector used to read the weight of a load. One of the operations of the Load Cell is to read the weight of the water per gallon in the automatic refilling of the drinking water system. The system uses a Load Cell Detector with a Kalman Filter System to ameliorate the reading process before the control system input. Also, the system is streamlined by adding a coin acceptor as means of sale to grease the guests when refilling. This streamlined system applies single load cells which occasionally get inaccurate and unstable readings of the gallon weight. To overcome these short appearances, an exploration is conducted aiming to establish a system to read the gallon weight more accurately and more stable. This is done by applying a full ground load cell and Kalman Filter which will ameliorate the input signal system. This control system will automatically stop the drinking water refilling by the time it reaches a weight equal to 19-liter water. After conducting tests, the crimes of refilling 2 gallons of drinking water without using a Kalman Filter are 1.94% and 1.89% while after using Kalman Filter the crimes are 0.63% and 0.52%.*

***Keywords:*** *Full Bridge Load Cell, Kalman Filter, Noise*

**EMAIL**

abdulharits03@gmail.com
wildanpambudi.wp@gmail.com

**ABSTRAK**

Load Cell adalah sensor yang digunakan untuk membaca berat suatu beban. Satu aplikasi load cell membaca gallon air untuk sistem pengisian air minum otomatis. Sistem sebelumnya menggunakan ruang berat yang dilengkapi dengan metode filter Kalman untuk meningkatkan proses pembacaan sebelum menerapkan sistem control. Kemudian, sistem tersebut diperluas dengan mesin kasir sebagai alat transaksi yang memudahkan konsumen untuk mengisi ulang air minum. Sistem ini menggunakan signle load cell, sehingga pembacaan berat gallon kurang akurat dan tidak konsisten. Berdasarkan kekurangan tersebut, tujuan dari penelitian ini adalah untuk membuat sistem pembacaan berat terpadu yang lebih akurat dan stabil, menggunakna load cell full-bridge dngan metode filter Kalman untuk meningkatkan sinyal input. Sistem control ini secara otomatis menghentikan penuangan air minum saat berat mencapai 19 liter. Setelah dilakukan pengujian penambahan 2 galon tanpa filter Kalman didapatkan hasil error 1,94% dan 1,89%, sedangkan menggunakan filter Kalman hasil error 0,63% dan 0,52%.

***Kata kunci****: Full Bridge Load Cell, Filter Kalman, Noise*

**PENERBIT**

Jurusan Teknik Elektro-ITATS
Alamat:
Jl. Arief Rachman Hakim No.100,Surabaya 60117,
Telp/Fax: 031-5997244

## PENDAHULUAN

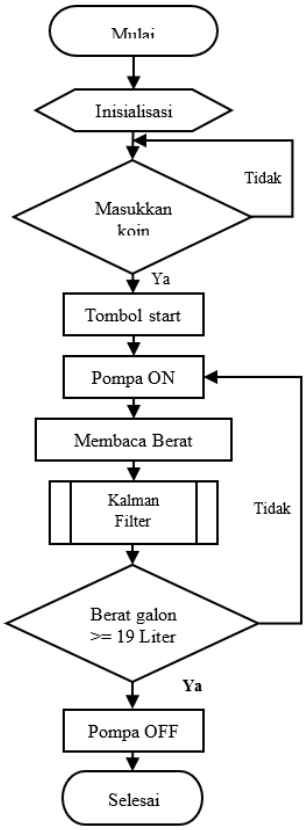
Air minum merupakan kebutuhan yang sangat vital untuk kehidupan manusia. Namun kondisi air minum di perkotaan saat ini semakin langka seiring sungai yang menjadi sumbernya mulai tercemar oleh berbagai macam limbah. Dari situlah mulai bermunculan banyak usaha depo pengisian air minum isi ulang, yang bisa didapatkan dengan harga yang lebih murah dibandingkan dengan air minum dalam kemasan. Dari sekian banyak usaha depo pengisian air minum isi ulang, terdapat sebuah permasalahan dimana depo yang masih melakukan pengisian dengan cara manual atau melakukan pengisian air minum dengan cara memperhatikan pengisian air minum hingga gallon terisi sesuai kapasitas. Dalam segi pelayanan, depo pengisian air minum isi ulang dituntut untuk melakukan sebuah peningkatan dalam hal melakukan pengisian secara praktis untuk memuaskan konsumen [1].

Dari permasalahan tersebut dibuat sistem dengan menggunakan coin acceptor sebagai media transaksi pembayaran dengan hanya membawa uang koin yang dapat mempermudah konsumen untuk melakukan pengisian air minum. Kemudian dengan menerapkan full bridge load cell yang berguna sebagai penerima data pembacaan berat yang digunakan sebagai parameter penuh atau tidaknya gallon air, dari pembacaan berat gallon tersebut sistem akan menghentikan pengisian gallon air sudah terisi penuh. Dan dengan menggunakan metode Kalman Filter yang akan mereduksi noise saat pengisian air minum yang disebabkan tekanan air dari kran saat pengisian.

## METODE PENELITIAN

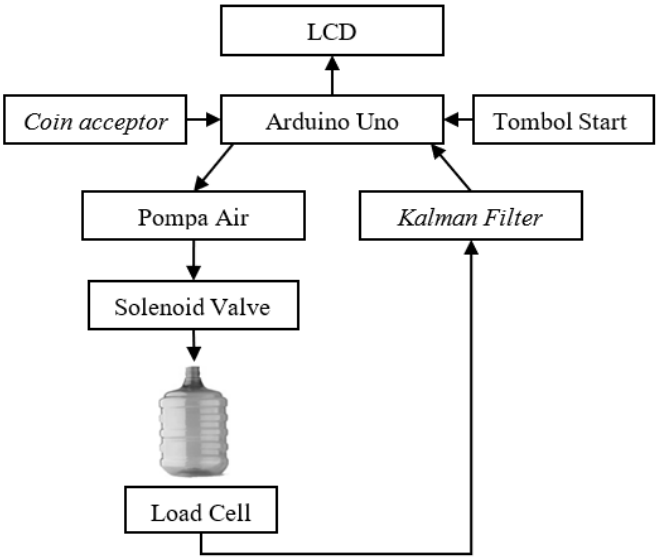
### Desain Sistem

Ketika *Coin Acceptor* sudah terisi uang koin sesuai dengan yang ditentukan, maka tombol *Start* siap ditekan untuk mengaktifkan otomasi pengisian gallon air isi ulang, dan setelah tombol ditekan, pompa air akan aktif untuk mengisi gallon air hingga berat yang dibaca sesuai dengan ketentuan 19 liter. Bila air gallon sudah tercapai 19 liter, maka pompa air akan mati. Namun apabila isi gallon air masih belum mencapai 19 liter maka air akan mengisi terus gallon air isi ulang tersebut hingga yang terbaca oleh sensor *Load Cell* sebesar 19 liter. Hasil dari pengisian air ini masih terdapat banyak *Noise* maka dari itu diperlukan metode *Kalman Filter* agar mendapatkan hasil yang akurat agar mudah dibaca dari gangguan getaran saat pengisian air. Gambar 1 berikut ini menampilkan Diagram Alur dari Sistem penelitian.




**Gambar 1**. Flowchart Sistem Pengisian Air Minum Otomatis

Gambar 2 di bawah ini menunjukkan Blok Sistem Pengisian Air Minum Otomatis. Komponen utama penelitian ini terdiri dari Input berupa *Coin Acceptor* untuk mengaktifkan pengoperasian sistem, yang selanjutnya diproses oleh Arduino Uno sebagai unit pengolah dan Output.




**Gambar 2**. Blok Diagram Sistem Pengisian Air Minum Otomatis

## HASIL DAN PEMBAHASAN

### Pengujian Sistem Tanpa *Kalman Filter*

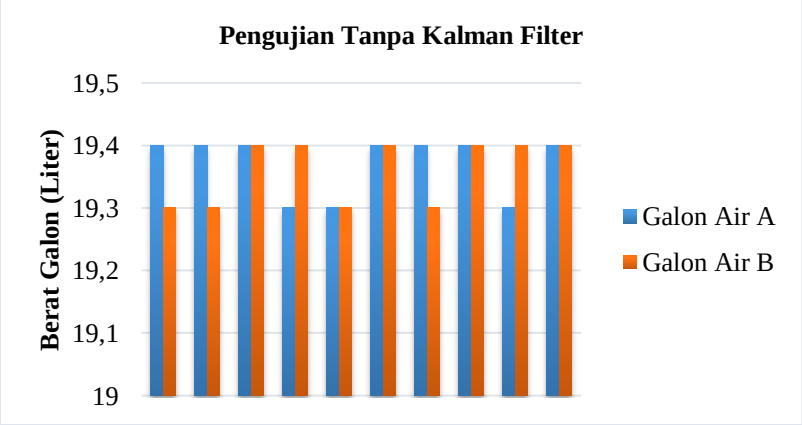
Pengujian ini dimaksudkan untuk mengetahui hasil dari pengisian gallon air sebanyak 10 kali tanpa Filter Kalman untuk memberikan perbandingan dengan menambahkan air gallon untuk selanjutnya dianalisa dengan Filter Kalman. Pengujian ini menjelaskan dimana sensor *Load Cell*

akan diuji mengisi gallon air dengan ukuran 19 liter dengan menggunakan pompa air untuk mengetahui seberapa besar gangguan getaran yang terjadi pada saat pengisian gallon air. Gangguan ini kemudian diproses dalam Filter Kalman, yang memudahkan pembacaan *Load Cell*.

Alat yang digunakan dalam pengujian adalah rangkaian pengisi air minum otomatis yaitu rangkaian *Coin Acceptor*, rangkaian *Full Bridge Load Cell*, rangkaian LCD, rangkaian Relay dengan pompa air dan Solenoid Valve, Power Supply 5V dan 12V, dan rangkaian Push Button. Tabel 1 berikut menampilkan Hasil Pengujian Otomatisasi Pengisian Air Minum tanpa Filter Kalman, sedangkan Gambar 3 menampilkan Diagram Batang Pembacaan Berat *Load Cell* tanpa Kalman Filter.

**Tabel 1**. Hasil Pengujian Otomatisasi Pengisian Air Minum tanpa *Filter Kalman* dan Ditimbang dengan Timbangan Digital

| Pengujian | Berat Ketentuan (Liter) | Galon Air A (Liter) | Galon Air B (Liter) |
|---|---|---|---|
| 1 | 19 | 19,4 | 19,3 |
| 2 | 19 | 19,4 | 19,3 |
| 3 | 19 | 19,4 | 19,4 |
| 4 | 19 | 19,3 | 19,4 |
| 5 | 19 | 19,3 | 19,3 |
| 6 | 19 | 19,4 | 19,4 |
| 7 | 19 | 19,4 | 19,3 |
| 8 | 19 | 19,4 | 19,4 |
| 9 | 19 | 19,3 | 19,4 |
| 10 | 19 | 19,4 | 19,4 |
| **Rata-Rata** | | 19,37 | 19,36 |
| **Error** | | 1,94 % | 1,89 % |




**Gambar 3**. Diagram Batang Pembacaan Berat Load Cell tanpa Kalman Filter

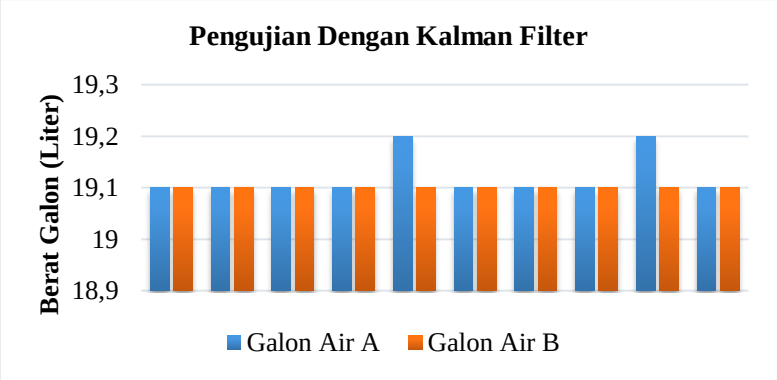
**Pengujian Sistem Menggunakan *Kalman Filter***

Pengujian ini adalah pengujian keseluruhan dari alat pengisian air minum isi ulang dengan sistem *Full Bridge Load Cell* dan *Kalman Filter* yang dimaksudkan untuk mengetahui hasil dari pengisian gallon air sebanyak 10 kali dengan menggunakan *Kalman Filter* dengan menggunakan 2 jenis gallon yang berbeda merek. Peralatan yang digunakan dalam pengujian ini yaitu rangkaian *Coin Acceptor*, rangkaian *Full Bridge Load* Cell dengan HX711, rangkaian LCD, rangkaian Relay pompa air dan Solenoid Valve, Power Supply 5V dan 12V, rangkaian Push Button dan *Kalman Filter*. Tabel 2 berikut menampilkan Hasil Pengujian Otomasi Pengisian Air Minum Isi Ulang dengan Kalman Filter, sedangkan Gambar 4 berikut menampilkan Diagram Batang Pembacaan Berat Load Cell dengan Kalman Filter.

**Tabel 2**. Hasil Pengujian Otomatisasi Pengisian Air Minum dengan *Filter Kalman* dan Ditimbang dengan Timbangan Digital

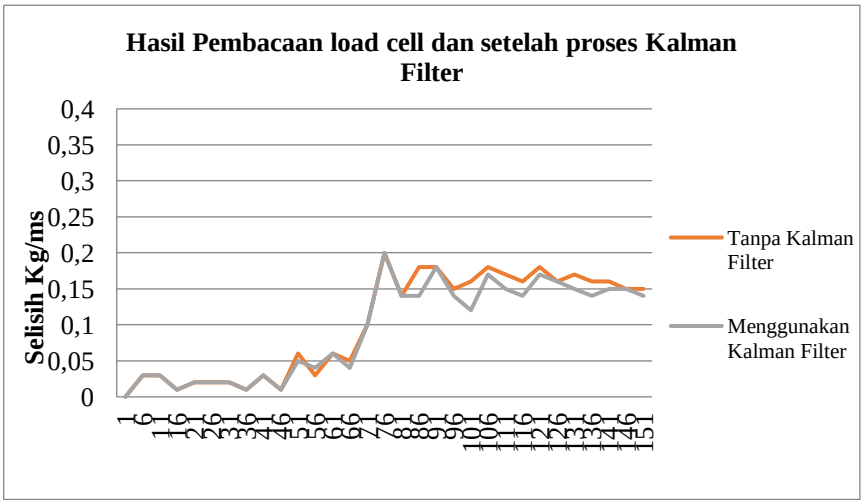
| Pengujian | Berat Ketentuan (Liter) | Galon Air A (Liter) | Galon Air B (Liter) |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | 19 | 19,1 | 19,1 |
| 2 | 19 | 19,1 | 19,1 |
| 3 | 19 | 19,1 | 19,1 |
| 4 | 19 | 19,1 | 19,1 |
| 5 | 19 | 19,2 | 19,1 |
| 6 | 19 | 19,1 | 19,1 |
| 7 | 19 | 19,1 | 19,1 |
| 8 | 19 | 19,1 | 19,1 |
| 9 | 19 | 19,2 | 19,1 |
| 10 | 19 | 19,1 | 19,1 |
| **Rata-Rata** | | 19,12 | 19,1 |
| **Error** | | 0,63 % | 0,52 % |




**Gambar 4**. Diagram Batang Pembacaan Berat Load Cell dengan Kalman Filter

Gambar 5 berikut merupakan Gambar Grafik dari Pengujian *Load Cell* ketika melakukan pengisian air minum isi ulang tanpa menggunakan *Kalman Filter* dan dengan menggunakan *Kalman Filter*. Pada Grafik bisa terlihat bahwa gangguan *Noise* yang muncul saat pengujian tanpa *Kalman Filter* dapat dikurangi dengan ketika menggunakan *Kalman Filter*.




**Gambar 5**. Hasil Pembacaan Sensor *Load Cell* Sebelum dan Sesudah proses *Kalman Filter*

## KESIMPULAN

Dari berat ketentuan yaitu sebesar 19 liter didapatkan hasil error dari pengujina 2 galon berbeda merk tanpa menggunakan Kalman Filter memberikan persentasi error 1,94% dan 1,89% dengan berat rata-rata masing-masing 19,37 liter dan 19,36 liter untuk tiap merk. Saat menguji seluruh sistem, yaitu mengisi tangki isi ulang air minum dengan Filter Kalman, tingkat kesalahan lebih baik daripada tanpa Filter Kalman. Persentasi error yang didapat saat pengujian dengan Filter

Kalman adalah 0,63% dan 0,52% dengan berat rata-rata masing-masing 19,12 liter dan 19,1 liter untuk tiap merek.

## DAFTAR PUSTAKA

[1] Suhendra, Imam dan Pambudi,Wahyu Setyo. 2015. "*Aplikasi Load Cell Untuk Otomasi Pada Depo Air Minum Isi Ulang"*. Jurnal Saint Dan Informatika. Kalimantan Selatan.

[2] Rudiyanto, B. I. Setiawan, and S. K. Saptomo. 2006. Algoritma *Kalman Filter* untuk Penghalusan Data. *Jurnal Keteknikan Pertanian*. Vol. 20, No. 3, Page: 287~292.

[3] Kitoma. 2015. Load Cell dan Timbangan. Indonesia.

[4] Welch. G, Bishop. G. 2006. " *An Introduction to the Kalman Filter*", Departement of Computer Science University of North Carolina at Chapter Hill.

[5] Electronics.stackexchange, "How to set up load cell sensor in a full bridge with amplifier", [Online].
Available: https://electronics.stackexchange.com/how-to-set-up-load-cell-sensor-in-a-full-bridge-with-amplifier. [Accesed: 20-Jun-2017].

JREEC
JOURNAL RENEWABLE ENERGY ELECTRONICS AND CONTROL
homepage URL : https://ejurnal.itats.ac.id/jreec

# Analisa Kinerja Minyak Trafo Berdasar Hasil Uji *Dissolved Gas Analysis* (DGA) Dengan Metode *Total Dissolved Combustible Gas* (TDCG) Di PLTU MUARA KARANG

*Mahmud Ansori*

*Institut Teknologi Adhi Tama Surabaya (ITATS)*

*e-mail: hita@itats.ac.id*

**INFORMASI ARTIKEL**

Jurnal JREEC – Volume03
Nomer 01, Juni 2023

Halaman:
27 – 34
Tanggal Terbit :
06 Juni 2023

DOI:
10.31284/j.JREEC.2023.v31i.4510

***ABSTRACT***

Transformer is a device used to increase or decrease an AC voltage without any change in power. Not only main transformers are needed, but Auxilary transformers are very important as well. The method for identifying and analyzing gas dissolved in transformer oil is referred to as the DGA (Dissolved Gas Analysis) method. In this study, it identified the performance of transformer oil (Reverse Auxilary Transformer 3 & 4 PLTU MUARA KARANG). IEEE std standard. C57 - 104.2008 is used as a benchmark for the analysis of test results from the DGA. The analysis method used Four methods are the Key Gas Method, the Roger Rat io Method and the Dvual triangle Method, and the TDCG (Total Dissolved Combustible Gas) Method . The calculation of the performance index of RAT 3 using the Key Gas Method, which gets a result of 90% : 10%. Then the Roger ratio method is Case 4 which is (Thermal <700 °C). The next method is Dvual triangle transformer oil conditions are at T3, T2 and T1. In the TDCG Analysis method, namely in condition 1, where transformer oil works optimally. Towards RAT 4 the key gas method shows a ratio of 82% : 7%. With Roger ratio conditions namely PD, T1 ,and T3. TDCG method the result of this DGA test is in condition 1, where this condition is a normal operating condition for minyak transformer. That the condition of the transformer oil RAT 3 & 4 is Normal Operation according to its parameters.

Key word : Reverse Auxilary Transformator 3&4 , Dissolved Gas Analysis , TDCG

**EMAIL**

Email Penulis 1
Email Penulis 2
Email Penulis … – font 9

**PENERBIT**

Jurusan Teknik Elektro-ITATS
Alamat:
Jl. Arief Rachman Hakim No.100,Surabaya 60117,
Telp/Fax: 031-5997244



**ABSTRAK**

Trafo adalah alat yang digunakan untuk menambah atau mengurangi tegangan AC tanpa ada perubahan daya. Metode untuk mengidentifikasi dan menganalisis gas yang terlarut dalam minyak transformator disebut sebagai metode DGA (Dissolved Gas Analysis). Pada penelitian ini diidentifikasi kinerja minyak trafo (Reverse Auxilary Transformer 3 & 4 PLTU MUARA KARANG). Standar STD IEEE. C57 - 104.2008 digunakan sebagai patokan untuk analisis hasil pengujian dari DGA. Metode analisis yang digunakan Empat metode adalah Metode Key Gas, Metode Roger Rat io dan Metode Dvual triangle , dan Metode TDCG (Total Dissolved Combustible Gas). Perhitungan indeks kinerja RAT 3 menggunakan Metode Key Gas, yang mendapatkan hasil 90% : 10%. Maka metode Roger ratio adalah Case 4 yaitu (Thermal <700 °C). Metode selanjutnya adalah kondisi oli transformator segitiga Dvual berada di T3, T2 dan T1. Pada metode TDCG Analysis yaitu pada kondisi 1, dimana oli trafo bekerja secara optimal. Terhadap RAT 4 metode key gas menunjukkan rasio 82% : 7%. Dengan kondisi rasio Roger yaitu PD, T1 ,dan T3. Metode TDCG hasil uji DGA ini berada pada kondisi 1, dimana kondisi ini merupakan kondisi operasi normal untuktrafo minyak. Bahwa kondisi oli trafo RAT 3 & 4 adalah Normal Operation sesuai parameternya.

Kata kunci: Reverse Auxilary Transformator 3&4, Analisis Gas Terlarut, TDCG

**PENDAHULUAN – font 11**

Salah satu penyebab utama munculnya kegagalan pada trafo adalah adanya panas yang berlebih, sehingga menimbulkan reaksi berantai yang akan mempercepat penurunan usia dan kualitas kerja sistem isolasi[1][2]. Kertas selulosa dan minyak trafo merupakan pelindung bagian dalam trafo dan untuk mengetahui kerusakan pada trafo dengan menguji jenis proteksi khususnya oli trafo[3]. Karena Oli trafo digunakan untuk menahan tegangan putus dan mengurangi intensitas yang dihasilkan[4], sehingga trafo dapat terlindungi dari impedansi. Karena saat terjadi impedansi akan mengakibatkan penurunan lifetime, sehingga kinerja trafo menjadi tidak maksimal[5]. Untuk itu perlu dilakukan pengujian kandungan gas pada oli trafo (uji Dissolved Gas Analysis), yang bertujuan memeriksa kondisi trafo berdasarkan banyaknya gas yang terdisintegrasi dalam minyak trafo[4][6]dan dampak kenaikan kandungan gas tercampur dalam minyak trafo. Berdasarkan permasalahan yang ada dan hasil uji kualitas dari minyak trafo, maka penelitian membahas tentang Kinerja Minyak Trafo berdasar hasil Uji Dissolved Gas Analysis (DGA) menggunakan Metode Analisa TDGC (Total Dissolved Combustible Gas) di PLTU Muara Karang, yang bertujuan untuk mengantisipasi ketahanan dari minyak trafo di PLTU Muara Karang terhadap pengaruh gas terlarut (CO, $H2$, $CH4$, $C2H6$, $C2H4$, dan $C2H2$).

**TINJAUAN PUSTAKA**

**Transformator**

Merupakan alat elektromagnetik yang sederhana, andal dan efisien untuk mengubah tegangan AC dari satu tingkat ke tingkatan yang lain dan berfungsi untuk menyalurkan daya atau energi listrik dari tegangan tinggi ke tegangan rendah atau sebaliknya serta digunakan untuk menaikkan atau menurunkan tegangan[7].

**Mintak Transformator**

Merupakan minyak mineral yang diperoleh dengan penyulingan dari minyak mentah, berfungsi sebagai pendingin karena minyak transformator mampu menghantarkan panas dengan baik dan sebagai isolaror yang baik agar dapat menjadi pemisah tegangan antara bagian-bagian yang memiliki beda fasa [8] [9], harus mempunyai kriteria: Kejernihan, Massa jenis, Tingkat kekentalan, Titik nyala , Titik tuang, Angka kenetralan, korosi belerang, tegangan tembus, faktor kebocoran dielektrik, Stabilitas (oxydation stability), kandungan air, tahanan jenis, tegangan permukaan, kandungan gas.

**Kekuatan Dielektrik**

Merupakan ukuran kemampuan suatu material untuk dapat menahan medan elektrik tanpa berakibat terjadinya tembus listrik pada material isolasi tersebut. Kekuatan dielektrik dipengaruhi oleh material dari elektroda, suhu, jenis tegangan yang diberikan, gas yang terdapat dalam cairan, dan sebagainya yang dapat merubah sifat molekul cairan. Dalam isolasi cair kekuatan dielektrik setara dengan tegangan yang terjadi[10]. Seperti pada hukum Paschen, kekuatan dielektrik suatu fluida sekitar 107 V/cm dan dapat menempati volume ruangan yang seharusnya dilindungi dan sekaligus dapat menyebarkan panas yang ditimbulkan oleh konveksi[11].

**Pengujian Isolasi Trafo**

Penyebab kegagalan isolasi diantaranya partikel padat, uap air dan gelembung gas didalamnya, proteksi yang sudah cukup lama digunakan, penurunan kekuatan dielektrik dan proteksi yang memiliki tegangan lebih[12]. Dengan metode Dissolved Analysis Gas (DGA), Uji karakteristik dielektrik, Furan analisis, BDV, Inspeksi peralatan, Visual inspeksi, Uji factor daya dan riwayat pembebanan dari trafor itu sendiri[13].

**Dissolved Gas Analysis (DGA)**

Pada saat transformator beroperasi akan menyebabkan minyak trafo mengalami pembebanan yang berupa beban elektris dan termal[14], kondisi dimana transformator dilihat dari hasil perhitungan jumlah gas terlarut pada minyak trafo. Jumlah gas terlarut yang mudah tersebut akan menunjukkan apakah transforamator yang diuji masih dalam kondisi normal, waspada atau kondisi kritis[15].

Ada 4 kriteria tingkatan kondisi untuk mengklasifikasikan kondisi trafo, dari hasil pengujian dilakukan interpretasi data hasil pengujian.

1. **Metode Key Gas**

Sebagai gas-gas yang terbentuk pada trafo berdasarkan jenis gas yang khas atau lebih dominan terbentuk pada temperature yang menghasilkan indikasi gas tertentu[13].

2. **Metode Roger Ratio**

Untuk menganalisis indikasi kegagalan menggunakan empat perhitungan gas rasio dari lima jenis gas yang dihitung untuk menentukan tipe kegagalan yang terjadi, Gas-gas yang digunakan adalah $C_2H_2/C_2H_4$, $CH_2/H2$, $C_2H_4/C_2H_6$.

3. **Metode Dvual Triangle**

Memaparkan hasil perhitungan analisis terkait dengan konsentrasi gas yang terlarut yang ditentukan oleh tiga jenis gas $CH_4$, $C_2H_4$ dan $C_2H_2$[14] dan digunakan untuk membentuk metode-metode analisis yang lain.

4. **Metode TDCG**

Ketika terjadi peningkatan dalam kandungan gas terlarut dari minyak trafo yang berhasil beroperasi terjadi dan diduga terjadi gangguan internal, untuk menghitung nilai TDCG dengan menjumlahkan nilai $H_2$, $CH_4$, $C_o$, $C_2H_2$, $C_2H_4$, $C_2H_6$ dalam satuan ppm[1].

**METODE**

Penelitian dilakukan di PT.PJB PLTU Muara Karang, yang terkait kinerja minyak transformator pada Transformator RAT (Reverse Auxilary Transformator) 3 dan 4 berdasarkan standar IEEE Std C57.104-2008. Pengujian DGA dilakukan berdasarkan:


Gambar 1. Diagram Alir Penelitian

## HASIL DAN PEMBAHASAN

### 1. Hasil Uji Dissolved Gas Analysis RAT 3

#### a. Metode Key Gas

Nilai Key Gas total = $H_2 + CH_4 + C_o + C_2H_2 + C_2H_4 + C_2H_6$
= 0 + 0 + 11 + 0 + 0 + 2
= 13 ppm

nilai % $C_o = \frac{11}{13}$ x 100% = 85%

Tabel 1. Hasil Perbandingan Uji DGA dengan standar IEEE

| Tanggal | $H_2 : C_2H_2$ (%) | $H_2 : CH_4$ (%) | $C_2H_6 : C_2H_4$ (%) | *CO* (%) |
|---|---|---|---|---|
| 27-Apr-18 | 0% : 0% | 0% : 0% | 15% : 0% | 85% |
| 03-Sep-18 | 13% : 0% | 13% : 8% | 19% : 2% | 57% |
| 02-Jul-19 | 16% : 0% | 16% : 0% | 18% : 2% | 63% |
| 30-Jun-20 | 12% : 0% | 12% : 1% | 17% : 1% | 68% |
| 15-Apr-21 | 0% : 0% | 0% : 0% | 90% : 10% | 0% |
| 03-Jun-21 | 10% : 0% | 10% : 2% | 11% : 3% | 75% |
| 31-Dec-21 | 4% : 0% | 4% : 17% | 33% : 3% | 44% |

Berdasarkan tabel 1, nilai hasil uji DGA pada RAT 3 terjadi Overheating of oil yang disebabkan oleh kenaikan dari gas Ethana yang melebihi standar IEEE C57-104.2008 sebesar 90% : 10% yang mendominasi adalah Ethana $C_2H_6$ mencapai 90%.

#### b. Metode Roger Ratio

Ratio 1 ($R_1$) = $\frac{CH_4}{H_2}$ = $\frac{0}{11}$ = 0,64 *Ppm*

Tabel 2. Hasil Uji DGA metode Roger Ratio

| Tanggal | R1 ($CH_4/H_2$) *(Ppm)* | R2 ($C_2H_2/C_2H_4$ ) *(Ppm)* | R5 ($C_2H_4/C_2H_6$) *(Ppm)* |
|---|---|---|---|
| 27-Apr-18 | ∞ | ∞ | 0,00 |
| 03-Sep-18 | 0,64 | 0 | 0,13 |
| 02-Jul-19 | 0 | 0 | 0,13 |
| 30-Jun-20 | 0,11 | 0 | 0,08 |
| 15-Apr-21 | ∞ | 0 | 0,11 |
| 03-Jun-21 | 0,16 | 0 | 0,24 |
| 31-Dec-21 | 4,38 | 0 | 0,10 |

Berdasarkan tabel 2, pada tanggal 31 Desember 2021 hasil $R_1$ $(CH_4/H_2)$ dengan Thermal <700 °C menunjukkan bahwa minyak transformator bekerja lebih berat dari pada biasanya. Hal ini dikarenakan gas Methana mulai terbentuk lebih banyak dari pada sebelumnya.

#### c. Metode Dvual Triangle

Nilai total Dvual tiangle = $CH_4 + C_2H_4 + C_2H_2 = 0 + 0 + 0 = 0\ ppm$

nilai % $C_2H_2$ = $\frac{100x}{Nilai\ total\ Dvual's\ Triangle} = \frac{0}{9}x100\% = 0\%$

Tabel 3. Hasil Uji DGA metode Dvual Triangle

| Tanggal | Nilai total Dvual triangle **(***Ppm***)** | $C_2H_4$ (%) | $CH_4$ (%) | $C_2H_2$ (%) | Kondisi |
|---|---|---|---|---|---|
| 27-Apr-18 | 0 | 0% | ∞ | ∞ | Normal |
| 03-Sep-18 | 9 | 22% | 78% | 0% | T2 |
| 02-Jul-19 | 3 | 100% | 0% | 0% | T3 |
| 30-Jun-20 | 4 | 50% | 50% | 0% | T3 |
| 15-Apr-21 | 7 | 100% | 0% | 0% | T3 |
| 03-Jun-21 | 8 | 63% | 38% | 0% | T3 |
| 31-Dec-21 | 42 | 17% | 83% | 0% | T1 |

Berdasarkan tabel 3 hasil pengujian DGA pada kondisi T2 terjadi panas berlebih ( 300 – 700 °C), T3 melebihi >700 °C. Kondisi tersebut menunjukkan bahwa minyak trafo bekerja pada suhu yang tinggi dikisaran > 300°C sampai >700 °C.

**d. Metode TDCG**

Nilai TDCG = $CO+H_2+CH_4+ C_2H_6+C_2H_4+ C_2H_2$ = 11 + 0 + 0 + 2 + 0 + 0 = 13 *Ppm*

Tabel 4. Hasil Uji DGA metode TDCG

| Tanggal | $H_2$ (*Ppm*) | $CH_4$ (*Ppm*) | $C_2H_6$ (*Ppm*) | $C_2H_4$ (*Ppm*) | $C_2H_2$ (*Ppm*) | *CO* (*Ppm*) | TDCG (*Ppm*) | Kondisi |
|---|---|---|---|---|---|---|---|---|
| 27-Apr-18 | 0 | 0 | 2 | 0 | 0 | 11 | 13 | 1 |
| 03-Sep-18 | 11 | 7 | 16 | 2 | 0 | 47 | 83 | 1 |
| 02-Jul-19 | 20 | 0 | 23 | 3 | 0 | 79 | 125 | 1 |
| 30-Jun-20 | 19 | 2 | 26 | 2 | 0 | 106 | 155 | 1 |
| 15-Apr-21 | 0 | 0 | 63 | 7 | 0 | 0 | 70 | 1 |
| 03-Jun-21 | 19 | 3 | 21 | 5 | 0 | 141 | 189 | 1 |
| 31-Dec-21 | 8 | 35 | 68 | 7 | 0 | 91 | 209 | 1 |

Berdasarkan tabel 4 hasil akhir dengan metode TDCG pada kondisi 1, dimana kondisi tersebut menjelaskan bahwa transformator beroperasi pada kondisi normal.

**2. Hasil Uji Dissolved Gas Analysis RAT 4**

**a. Metode Key Gas**

Nilai Key Gas total = $H_2+ CH_4 + C_o + C_2H_2 + C_2H_4 + C_2H_6$
= 10 + 0 + 0 + 0 + 7 + 78
= 95 ppm

nilai % $C_o = \frac{0}{95}$ x 100% = 0%

Tabel 5. Hasil Perbandingan Uji DGA dengan standar IEEE

| Tanggal | $H_2 : C_2H_2$ (%) | $H_2 : CH_4$ (%) | $C_2H_6 : C_2H_4$ (%) | *CO* (%) |
|---|---|---|---|---|
| 15-Mar-18 | 11% : 0% | 11% : 0% | 82% : 7% | 0% |
| 03-Sep-18 | 0% : 0% | 0% : 11% | 17% : 1% | 71% |
| 02-Jul-19 | 5% : 0% | 5% : 10% | 16% : 2% | 67% |
| 30-Jan-20 | 0% : 0% | 0% : 11% | 20% : 0% | 70% |
| 30-Jun-20 | 5% : 0% | 5% : 10% | 15% : 1% | 69% |
| 15-Apr-21 | 0% : 0% | 0% : 0% | 88% : 12% | 0% |
| 03-Jun-21 | 4% : 0% | 4% : 10% | 14% : 0% | 72% |
| 03-Dec-21 | 0% : 0% | 0% : 11% | 18% : 0% | 71% |

Berdasarkan tabel 5, nilai hasil uji DGA pada RAT 4 terjadi Overheating of oil yang disebabkan oleh kenaikan dari gas Ethana yang melebihi standar IEEE C57-104.2008 sebesar 90% : 10% yang mendominasi adalah Ethana $C_2H_6 : C_2H_4$ mencapai 90%.

**b. Metode Roger Ratio**

Ratio 1 ($R_1$) = $\frac{CH_4}{H_2}$ = $\frac{0}{10}$ = 0 *Ppm*

Tabel 6. Hasil Uji DGA metode Roger Ratio

| Tanggal | R1 ($CH_4/H_2$) (*Ppm*) | R2 ($C_2H_2/C_2H_4$) (*Ppm*) | R5 ($C_2H_4/C_2H_6$) (*Ppm*) |
|---|---|---|---|
| 15-Mar-18 | 0 | 0 | 0,09 |
| 03-Sep-18 | ∞ | 0 | 0,07 |
| 02-Jul-19 | 2 | 0 | 0,11 |
| 30-Jan-20 | ∞ | ∞ | 0 |
| 30-Jun-20 | 1,95 | 0 | 0,08 |
| 15-Apr-21 | ∞ | 0 | 0,13 |
| 03-Jun-21 | 2,33 | 0 | 0,03 |
| 03-Dec-21 | ∞ | ∞ | 0 |

Berdasarkan tabel 6, pada tanggal 31 Desember 2021 hasil $R_1$ ($CH_4/H_2$) berada pada Case 3 (temperature panas yang rendah), Kondisi ini juga dapat menyebabkan Gas Methana mulai terbentuk lebih banyak dari pada sebelumnya.

**c. Metode Dvual triangle**

Mencari nilai Dvual's Triangle total = $CH_4 + C_2H_4 + C_2H_2$ = 0 + 7 + 0 = 7 *Ppm*

Mencari nilai % $C_2H_2$ = $\frac{100_X}{Nilai\ total\ Dvual's\ Triangle} = \frac{0}{7} x100\% = 0\%$

Tabel 7. Hasil Uji DGA metode Dvual triangle

| Tanggal | Nilai total Dvual triangle (*Ppm*) | $C_2H_4$ (%) | $CH_4$ (%) | $C_2H_2$ (%) | Kondisi |
|---|---|---|---|---|---|
| 15-Mar-18 | 7 | 100% | 0% | 0% | T3 |
| 03-Sep-18 | 49 | 10% | 90% | 0% | T1 |
| 02-Jul-19 | 47 | 15% | 85% | 0% | T1 |
| 30-Jan-20 | 6 | 0% | 100% | 0% | PD |
| 30-Jun-20 | 48 | 10% | 90% | 0% | T1 |
| 15-Apr-21 | 2 | 100% | 0% | 0% | T3 |
| 03-Jun-21 | 44 | 5% | 95% | 0% | T1 |
| 03-Dec-21 | 9 | 0% | 100% | 0% | PD |

Berdasarkan tabel 7 hasil pengujian DGA pada kondisi PD menunjukkan bahwa terjadi pelepasan energi yang menyebabkan terjadinya lonjakan bunga api (arching). Kondisi T2 terjadi panas berlebih ( 300 – 700 °C), T3 melebihi >700 °C. Kondisi tersebut menunjukkan bahwa minyak trafo bekerja pada suhu yang tinggi dikisaran > 300°C sampai >700 °C.

**d. Metode TDCG**

Nilai TDCG = $CO+H_2+CH_4+ C_2H_6+C_2H_4+ C_2H_2$ = 0 + 10 + 0 + 78 + 7 + 0 = 95 Ppm

Tabel 8. Hasil Uji DGA metode TDCG

| Tanggal | $H_2$ $(Ppm)$ | $CH_4$ $(Ppm)$ | $C_2H_6$ $(Ppm)$ | $C_2H_4$ $(Ppm)$ | $C_2H_2$ $(Ppm)$ | $CO$ $(Ppm)$ | Nilai TDCG $(Ppm)$ | Kondisi |
|---|---|---|---|---|---|---|---|---|
| 27-Apr-18 | 0 | 0 | 2 | 0 | 0 | 11 | 13 | 1 |
| 03-Sep-18 | 11 | 7 | 16 | 2 | 0 | 47 | 83 | 1 |
| 02-Jul-19 | 20 | 0 | 23 | 3 | 0 | 79 | 125 | 1 |
| 30-Jun-20 | 19 | 2 | 26 | 2 | 0 | 106 | 155 | 1 |
| 15-Apr-21 | 0 | 0 | 63 | 7 | 0 | 0 | 70 | 1 |
| 03-Jun-21 | 19 | 3 | 21 | 5 | 0 | 141 | 189 | 1 |
| 31-Dec-21 | 8 | 35 | 68 | 7 | 0 | 91 | 209 | 1 |

Berdasarkan tabel 8 hasil akhir dengan metode TDCG pada kondisi 1, dimana kondisi tersebut menjelaskan bahwa transformator beroperasi pada kondisi normal.

## KESIMPULAN

Berdasarkan hasil pengujian DGA untuk RAT 3 dan 4 dengan metode Key gas, Roger ratio, Dvual triangle dan TDCG sesuai dengan standar IEEE C57-104.2008 kinerja minyak trafo masih normal untuk beroperasi

## DAFTAR PUSTAKA

[1] S. Ariyani, "Analisis Dissolved Gas Analysis Dan Klasifikasi Tipe Fault Pada Minyak Trafo Dengan Metode Naive Bayes Classifier Pada Transformator Daya 150 kV," *J. Tek. Elektro dan Komputasi*, vol. 1, no. 1, pp. 36–45, 2019, doi: 10.32528/elkom.v1i1.2181.

[2] A. Maruf and Y. Primadiyono, "Analisis Pengaruh Pembebanan Dan Temperatur Terhadap Susut Umur Transformator Tenaga 60 Mva Unit 1 Dan 2 Di Gi 150 Kv Kalisari," *Edu Elektr. J.*, vol. 10, no. 1, pp. 1–10, 2021.

[3] R. Oktaviani, Y. M. Simanjutak, and M. G. C. Portable, "ANALISIS PENGUJIAN DGA MENGGUNAKAN METODA CHROMATOGRAPHY GAS SEBAGAI INDIKASI KEGAGALAN MINYAK ISOLASI TRANSFORMATOR GI 150 KV KOTA BARU," *J. Tek. Elektro Univ. Tanjungpura*, vol. 20, 2020, [Online]. Available: https://jurnal.untan.ac.id/index.php/jteuntan/article/view/42556.

[4] J. Jumardin, J. Ilham, and S. Salim, "Studi Karakteristik Minyak Nilam Sebagai Alternatif Pengganti Minyak Transformator," *Jambura J. Electr. Electron. Eng.*, vol. 1, no. 2, pp. 40–48, 2019, doi: 10.37905/jjeee.v1i2.2881.

[5] Zhou, Yang, and Wang, "PERFORMANCE ANALYSIS OF STEP DOWN TYPE-TRANSFORMATOR OF FACTORIES AT THE COMPANY OF SURYA TOTO INDONESIA CIKUPA," *file:///C:/Users/VERA/Downloads/ASKEP_AGREGAT_ANAK_and_REMAJA_PRINT.docx*, vol. 21, no. 1, pp. 1–9, 2020.

[6] N. Fithri, J. R. Auliya, J. Jend, A. Yani, and N. Palembang, "ANALISIS KEGAGALAN ISOLASI MINYAK TRANSFORMATOR 27 MVA PLTG 1 JAKABARNG Berdasarkan Hasil Uji DGA," 2008.

[7] P. Studi, P. Teknik, F. Teknik, and U. N. Jakarta, *PENGARUH SUHU TERHADAP TEGANGAN TEMBUS MINYAK TRANSFORMATOR JENIS MINERAL*. 2017.

[8] H. Sayogi, "Analisis Mekanisme Kegagalan Isolasi Pada Minyak Trafo Menggunakan Elektroda Berpolaritas Berbeda Pada Jarum-Bidang Hanung Sayogi L2F302486 Teknik Elektro Universitas Diponegoro Semarang."

[9] U. L. Negara, "SPLN 491-2:19EtP," 1982.

[10] F. R. A. Bukit, "Analisis Kekuatan Dielektrik Minyak Campuran Metil Ester Bunga Matahari Sebagai Isolasi Cair Pada Transformator," *J. Energy Electr. Eng.*, vol. 3, no. 1, pp. 1–7, 2021, doi: 10.37058/jeee.v3i1.3650.

[11] O. E. Gouda, S. M. Saleh, and S. H. El-Hoshy, "Power transformer incipient faults diagnosis based on dissolved gas analysis," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 1, no. 1, pp. 10–16, 2016, doi: 10.11591/ijeecs.v1.i1.pp10-16.

[12] S. Bustamante, M. Manana, A. Arroyo, P. Castro, A. Laso, and R. Martinez, "Dissolved gas analysis equipment for online monitoring of transformer oil: A review," *Sensors (Switzerland)*, vol. 19, no. 19, pp. 4–12, 2019, doi: 10.3390/s19194057.

[13] A. Syakur, "Penerapan Metode Interpretasi Rasio Roger, Segitiga Duval, Breakdown Test, dan Water Content Test untuk Diagnosis Kelayakan Minyak Transformator," *Teknik*, vol. 40, no. 1, pp. 638–6, 2019, doi: 10.14710/teknik.v40n1.22056.

[14] T. Committee of the IEEE Power Engineering Society, *IEEE Std C57.14-2005, IEEE Guide for the Interpretation of Gases Generated in Silicone-Immersed Transformers*, vol. 2008, no. February. 2006.

[15] M. R. Hidayat *et al.*, "Analisis Kemampuan Minyak Isolasi Transformator Daya Merek Unindo Dengan Pengujian Dissolved Gas Analysis dan Breakdown Voltage di Gardu Induk Serpong," *Epsil. J. Electr. Eng. Inf.*, pp. 100–106, 2020.

JREEC
JOURNAL RENEWABLE ENERGY ELECTRONICS AND CONTROL
homepage URL : https://ejurnal.itats.ac.id/jreec

# Sistem Monitoring Kemacetan Lalu Lintas Di Kota Surabaya Berbasis Internet of Things (IoT)

HF Putranto[1], M Syamsul Huda[1], Ardylan Heri Kisyarangga[1] Roy Hamonangan Pardosi[1].
Jurusan Teknik Elektro – FTETI – Institut Teknologi Adhi Tama Surabaya[1]

*e-mail: hilman.f.putranto@gmail.com*

**INFORMASI ARTIKEL**

Jurnal JREEC – Volume 03
Nomer 01, Juni 2023

Halaman:
35 – 42
Tanggal Terbit :
06 Juni 2023

DOI:
10.31284/j.JREEC.2023v31i.4517

***ABSTRACT***

*The growth and development of the city of Surabaya are definitely closely related to population growth and an increase in the number of immigrants, which increases the number of motorized vehicles on the road. However, since the number of motorized vehicles has expanded faster than the capacity of the roads, traffic congestion has resulted. Congestion monitoring is designed to provide traffic density data to road users so that they can choose the best route to take at the appropriate time. This study describes a four-way junction with infrared sensors in each of the paths. As a vehicle detector, this infrared sensor is utilized. Tests on the prototype were conducted under a variety of typical traffic circumstances. This study makes use of an IoT prototype that is designed to be connected to the internet network so that users can view real-time traffic data from a distance. Firebase and an Android app are two of the informational tools utilized in this study. The study's findings suggest that the prototype can function effectively. The applied infrared sensor can operate at optimal efficiency at 1 cm - 4,5 cm and can precisely identify vehicles.*

***Keywords:*** *Traffic Congestion, Infrared, IoT, Firebase*

**EMAIL**

***hilman.f.putranto@gmail.com***
**royhamonangan54@gmail.com**
**rangga.gonggex95@gmail.com**
**syamsulhuda**

**PENERBIT**

Jurusan Teknik Elektro-ITATS
Alamat:
Jl. Arief Rachman Hakim No.100,Surabaya 60117,
Telp/Fax: 031-5997244



**ABSTRAK**

Pertumbuhan dan perkembangan kota Surabaya tentunya sangat erat kaitannya dengan pertumbuhan penduduk dan peningkatan jumlah pendatang yang meningkatkan jumlah kendaraan bermotor di jalan raya. Namun, karena peningkatan kapasitas jalan tidak secepat peningkatan jumlah kendaraan bermotor, maka terjadi kemacetan lalu lintas. Pemantauan kemacetan dirancang untuk memberikan data kepadatan lalu lintas kepada pengguna jalan sehingga mereka dapat memilih rute terbaik untuk diambil pada waktu yang tepat. Penelitian ini mendeskripsikan simpang empat arah dengan sensor infra merah di setiap jalurnya. Sebagai pendeteksi kendaraan, sensor infra merah ini digunakan. Pengujian pada prototipe dilakukan dalam berbagai keadaan lalu lintas yang khas. Penelitian ini memanfaatkan prototipe IoT yang dirancang untuk terhubung dengan jaringan internet sehingga pengguna dapat melihat data trafik secara realtime dari jarak jauh. Firebase dan aplikasi Android adalah dua alat informasi yang digunakan dalam penelitian ini. Temuan penelitian menunjukkan bahwa prototipe dapat berfungsi secara efektif. Sensor infra merah yang diterapkan dapat beroperasi dengan efisiensi optimal pada jarak 1 cm sampai 4,5 cm dan dapat mengidentifikasi kendaraan dengan tepat.

**Kata kunci:** Kemacetan Lalu Lintas, Inframerah, IoT, Firebase

## PENDAHULUAN – font 11

Kemacetan adalah situasi atau keadaan tersendatnya atau bahkan terhentinya lalu lintas yang disebabkan oleh banyaknya jumlah kendaraan melebihi kapasitas jalan. Kemacetan arus lalu lintas merupakan refleksi ketidakseimbangan kepadatan ruas jalur dalam menampung kendaraan yang melintas pada ruas jalur tersebut. Kemacetan kerap terjadi pada persimpangan yang ada rambu lampu lalu lintas [1].

Faktor pengaturan lampu lalu lintas yang belum fleksibel juga menjadi salah satu penyebab kemacetan. Pengaturan lalu lintas di Indonesia masih bersifat kaku dan tidak disesuaikan dengan tinggi rendahnya arus kendaraan. Akibatnya sering terjadinya antrian panjang yang menjadi awal kemacetan yang menyebabkan ketidakseimbangan di salah satu ruas persimpangan.

Internet of things atau bisa disingkat menjadi IoT adalah sebuah perkembangan di dalam bidang keilmuan yang sangat menjanjikan dikarenakan mengoptimalkan sebuah kehidupan berdasarkan sebuah sensor yang cerdas dan juga sebuah peralatan pintar yang saling bekerja-sama menggunakan sebuah jaringan dari internet [2].

Prototipe penelitian ini dibuat menggunakan empat sensor inframerah yang terbagi dalam empat ruas jalan dengan setiap ruas berisikan dua sensor inframerah sebagai sensor pendeteksi kemacetan. Konsep yang dibuat pada prototipe ini adalah Internet of Things (IoT), dimana prototipe akan terhubung dengan jaringan internet sehingga pengguna jalan dapat mengetahui kondisi lalu lintas secara real time.

Pada penelitian sebelumnya yang menggunakan mikrokontroller WEMOS D1 R32 dan platform ThinkSpeak serta Twitter. Hasil dari penelitian tersebut menunjukkan delay pada kecepatan jaringan dalam pengiriman tweet rata – rata adalah 18 detik. Nilai error pada delay pengiriman tweet yang didapatkan adalah 13% [3]. Selain monitoring lalu lintas, sistem monitoring jarak jauh juga sudah pernah digunakan dalam beberapa bidang antara lain kecepatan dan arah angin [4] serta trafo gardu distribusi [5].

Hasil dari penelitian ini yang menggunakan mikro kontroler ESP32 dan Firebase diharapkan dapat memberikan data kepadatan lalu lintas yang lebih baik kepada pengguna jalan, agar pengguna jalan dapat memilih rute terbaik yang akan dilalui pada waktu yang tepat.

## TINJAUAN PUSTAKA

### Penelitian Sebelumnya.

Penelitian terdahulu bertujuan untuk mendapatkan bahan perbandingan dan acuan. Selain itu, untuk menghindari anggapan kesamaan dengan penelitian ini. Maka dalam kajian pustaka ini peneliti mencantumkan hasil-hasil penelitian terdahulu. Pertama adalah Penelitian Rosyady, Phisca Aditya (2022), Penelitian ini merupakan prototipe yang menggambarkan persimpangan empat arah yang memiliki sensor inframerah di setiap jalurnya dan memanfaatkan konsep prototipe *Internet of things* (IoT) secara *realtime* mengunakan media informasi Twitter.

Hasil penelitian ini menunjukkan bahwa prototipe yang dibuat dapat bekerja dengan baik. Sensor inframerah yang digunakan dapat bekerja secara optimal dan dapat mendeteksi kendaraan secara tepat pada rentang sensitivitas 4,5 cm. Penundaan rata-rata dalam mengirim tweet notifikasi adalah 18 detik dan nilai error pada *delay* pengiriman tweet yang didapatkan adalah 13%. (Rosyady et al., 2022) Penelitian ini memiliki delay yang cukup signifikan karena adanya proses pelaporan data pada situs twitter.

Kedua adalah Penelitian yang dilakukan oleh BR, Nahdia Rupawanti (2019), Tujuan dari penelitian ini adalah untuk mendapatkan suatu sistem kontrol yang dapat mengurangi kemacetan-kemacetan di persimpangan yang terdapat sistem traffic light. Penelitian ini menggunakan metode penelitian kualitatif dan eksperimental. Mikrokontroller yang digunakan pada penelitian ini adalah ATMega328 dan sensor yang digunakan adalah sensor infrared. Hasil pengujian sensor infrared diperoleh nilai rata-rata 16 detik dan nilai rata-rata sensor light dependert resistor 66 detik. Dimana hasil dari penelitian ini ialah model desain rancang bangun berguna dalam pemanfaatan kesetabilan waktu tunggu infrared 16 detik – 20 detik sedangkan *light dependert resistor* 66 detik – 70 detik pada sistem traffic light. (Br, 2019) Penelitian ini masih belum berbasis IOT karena keterbatasan mikrokontroller yang digunakan.

Ketiga adalah Penelitian yang dilakukan oleh Dewi Indriasari (2017) Tujuan dari penelitian ini adalah (1) menganalisis tingkat kemacetan lalu lintas di daerah kajian; (2) menganalisis faktor dominan yang mempengaruhi terjadinya kemacetan lalu lintas di daerah kajian. Penelitian ini menggunakan metode survei dan observasi. Data primer dari penelitian ini berupa data volume lalu lintas, penggunaan lahan, tingkat kemacetan lalu lintas dan faktor dominan kemacetan lalu lintas. Data penggunaan lahan diperoleh dari interpretasi dan digitasi citra Ikonos yang mengacu pada klasifikasi penggunaan lahan Sutanto. Data volume lalu lintas diperoleh dari survei. Data tingkat kemacetan lalu lintas diperoleh dari perhitungan tingkat pelayanan jalan dan survei, sedangkan faktor dominan kemacetan diperoleh dari observasi kemacetan lalu lintas. Maka dari itu, kelemahan dari penelitian ini masih belum menggunakan system otomatis dikarenakan masih menggunakan metode survei dan observasi. (Indriasari, 2017)

Keempat adalah Penelitian yang dilakukan oleh Tri Apriyono, Dionisius P. Rumlus (2021) Tujuan dari penelitian ini adalah untuk mengetahui faktor-faktor yang mengakibatkan tingkat kemacetan lalu lintas pada ruas jalan Budi Utomo dan jalan Hasannudin Kota Timika dan untuk mengetahui faktor yang dominan mengakibatkan kemacetan lalu lintas pada ruas jalan Budi Utomo dan jalan Hasannudin di Kota Timika. Maka dari itu, kelemahan dari penelitian ini masih belum menggunakan system otomatis dikarenakan masih menggunakan metode survei dan observasi. (Apriyono and Rumlus, 2021)

Kelima adalah Penelitian yang dilakukan oleh Abdullah,luthfi rijalul Fikri (2018) Tujuan penelitian ini dirancang menggunakan mikrokontroler Atmega16, sensor kepadatan kendaraan, sensor penghitung jumlah kendaraan, tampilan LCD, tersedianya monitoring website yang di peruntukkan agar keadaan lalu lintas di jalan raya dapat termonitoring dengan baik, dan apabila terjadi pelanggaran atau masalah yang ada pada lalu lintas jalan dapat segera diatasi, tanpa harus lama sehingga dapat menimbulkan kemacetan. (Abdullah

and Fikri, 2018). Penelitian ini ada kelemahannya yaitu kurang tepatnya data terhadap real time yang telah diberikan.

Keenam adalah Penelitian (Porwal et al., 2021) yang menyajikan sistem kontrol dan pemantauan lampu lalu lintas berbasis kepadatan. Sistem ini berusaha mengurangi kemungkinan kemacetan lalu lintas, yang disebabkan oleh lampu lalu lintas, sampai batas tertentu. Sistem yang digunakan pada penelitian ini adalah MCS-51 family-berbasis mikrokontroller AT89S52 dan sensor yang digunakan adalah sensor Inframerah (IR).

Mikrokontroler membuat keputusan berdasarkan kepadatan jumlah kendaraan dan memperbarui waktu penundaan lampu lalu lintas. Lampu lalu lintas ditempatkan pada jarak tertentu dari sistem IR. Jadi berdasarkan jumlah kendaraan, mikrokontroler mendefinisikan rentang yang berbeda untuk penundaan lampu lalu lintas dan memperbaruinya. Hasil dari penelitian ini kepadatan lalu lintas masih hanya dapat dimonitor oleh pihak berwenang saja sehingga pengguna jalan umum masih belum dapat mengetahui kepadatan lalu lintas di persimpangan jalan yang akan dilewatinya.

Ketujuh adalah Penelitian yang dilakukan oleh Penelitian (Ramadhan et al., 2021) menggunakan mikrikontroler Arduino MEGA untuk membuat prototipe *smart traffic light controller* (STLC). Sensor yang digunakan adalah tiga sensor ultrasonic dan camera esp 32. Hasil dari penelitian ini menyarankan untuk mencapai sinkronisasi persimpangan tiga baris dan menerapkan keseimbangan antara jumlah kendaraan di setiap sisi dan lampu hijau. Ketika pelanggaran lalu lintas terjadi, kamera akan menangkap nomor mobil dan mengirimkannya ke database dengan menggunakan telegram. Penelitian ini terdapat inkonsisten pada abstrak.

Kedelapan adalah Penelitian yang dilakukan oleh Penelitian Pratiwi (2019) dengan tujuan untuk menganalisis penyebab kemacetan di jalan Kapasan dan Kenjeran, Kota Surabaya. Penelitian ini berjenis penelitian survei. Rancangan penelitian ini adalah cross sectional. Penentuan sampel menggunakan teknik accidental sampling. Sumber data berupa data primer dan data sekunder. Analisis data menggunakan analisis deskriptif. Teknik pengumpulan data observasi di lapangan dengan survei total counting menggunakan alat hand counter dan survei kebisingan menggunakan Decibel10th berdasarkan Keputusan Menteri Lingkungan Hidup No. KEP-48 / MENLH / 11/1996.

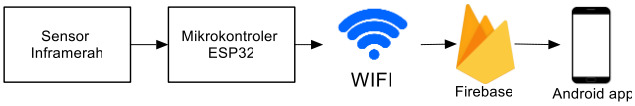
Hasil dari penelitian menunjukan bahwa di Jalan Kenjeran memiliki kapasitas jalan normal 2359,8 smp/jam tetapi pada hari senin dan rabu yang merupakan hari kerja dan hari masuk sekolah satuan mobil penumpang (SMP) jalan Kenjeran tertinggi mencapai 4495.39 smp/jam. Jalan Kapasan memiliki kapasitas normal 2010,2 smp jam. Penyebab kemacetan di Ruas Jalan Kapasan dan Jalan Kenjeran adalah 1)Pengguna jalan yang menggunakan bahu jalan untuk parkir, 2)Bongkar muat yang dilakukan pedagang disekitar

Ruas Jalan Kapasan-Kenjeran,3)Bertambahnya kendaraan pribadi setiap tahunnya membuat volume kendaraan tidak sesuai dengan kapasitas jalan.

Penelitian ini hanya mengumpulkan data dari salah satu ruas jalan di Kota Surabaya yang terdampak oleh kemacetan jalan. Menurut penulis salah satu saran untuk mengurai kemacetan adalah dengan menertibkan pedagang yang berada di pinggir jalan.

## METODE

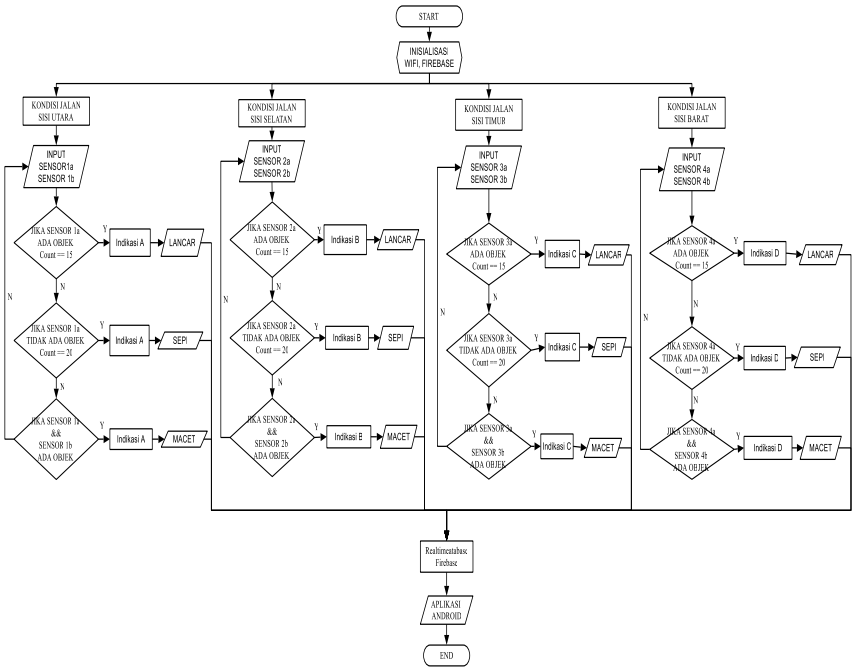
Penelitian ini dimulai dari studi literatur, kemudian perancangan sistem, analisa kebutuhan, implementasi dan pengujian. Pada Gambar 1 menunjukkan diagram blok sistem keseluruhan. Dari blok diagram sistem tersebut maka dapat diuraikan penjelasan bagian-bagian dari sistem dan cara kerjanya.




Gambar 1. Diagram Blok Sistem keseluruhan

Pada sistem yang dibangun, Mikrokontroler ESP32 digunakan sebagai pemroses utama, sedangkan sensor inframerah digunakan untuk mendeteksi halangan atau kendaraan pada prototipe. Pendeteksi halangan dengan sensor inframerah memanfaatkan prinsip pemantulan sinar inframerah. Transmiter pada modul inframerah akan memancarkan sinar inframerah dan kemudian diterima oleh receiver untuk mendapatkan letak objek dengan frekuensi yang sudah ditentukan pada IC LM393 dalam rangkaian modul sensor inframerah [6].

Data dari sensor akan dikirim ke internet dengan menggunakan platfrom Firebase, karena modul ESP32 sudah mendukung untuk terkoneksi dengan WiFi dan Bluetooth sehingga tidak memerlukan modul tambahan. Perancangan sistem deteksi kemacetan ini memanfaatkan platfrom Firebase untuk menyimpan data dan menampilkan informasi indikasi kemacetan kemudian akan ditampilkan kepada user pada android app.



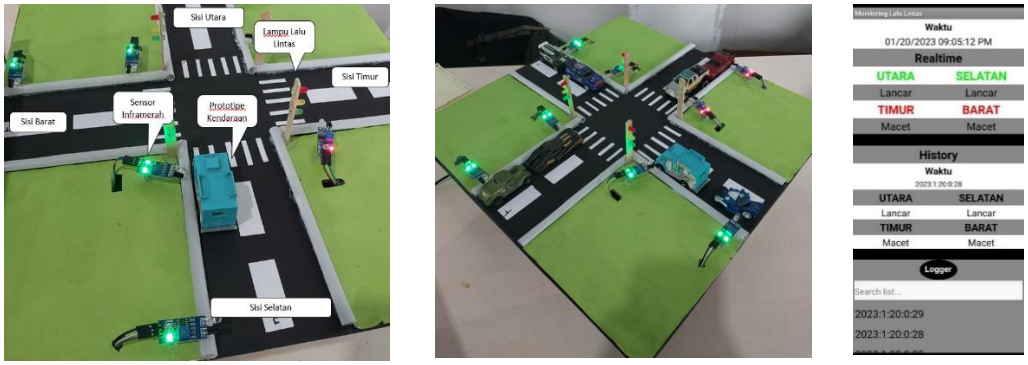

Gambar 2. Flowchart Software Sistem Monitoring Kemacetan Lalu Lintas

Berdasarkan diagram alir pada Gambar 2 terdapat proses awal yakni proses kondisi jalan pada setiap ruas jalan. Masing-masing proses dari setiap kondisi jalan diberikan masukan sensor inframerah berfungsi untuk mendeteksi kendaraan. Sensor inframerah bertanggung jawab untuk mengambil data. Data yang diambil hasilnya adalah berupa bilangan 0 (Low) dan 1 (High) karena pada dasarnya sensor inframerah merupakan sensor dalam kategori digital, dengan kondisi 1 tidak mendeteksi kendaraan dan apabila kondisi 0 maka akan mendeteksi kendaraan [7].

Setelah kendaraan terdeteksi maka dibuat kategori kondisi lalu lintas yakni Sepi, Normal dan Macet [8]. Untuk kondisi Sepi, sensor inframerah tidak mendeteksi kendaraan setelah Tiga detik. Kondisi Normal adalah kondisi ketika sensor inframerah mendeteksi adanya kendaraan setelah Enam detik. Terakhir untuk kondisi Macet adalah kondisi sensor inframerah mendeteksi adanya kendaraan setelah Sembilan detik. Apabila kondisi dari setiap jalan telah terpenuhi maka akan diproses dan diberikan label indikasi yakni 1 untuk kondisi Sepi, 2 untuk kondisi Normal dan 3 untuk kondisi Macet [9]. Setelah masing-masing jalan telah mendapatkan label indikasi maka akan dikirimkan pada server Firebase menggunakan jaringan WiFi yang tersedia dan ditampung pada RealtimeDatabase Firebase. Data yang telah ditampung pada RealtimeDatabase Firebase akan diteruskan pada Android app di smartphone pengguna.

## HASIL DAN PEMBAHASAN

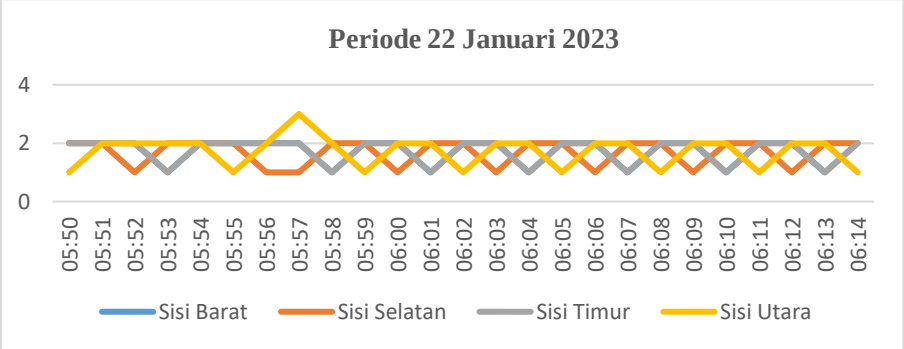
Perancangan prototipe monitoring kemacetan lalu lintas pada penelitian ini terlihat pada Gambar 3 (a) terdapat dua sensor di setiap sisi jalan. Jika kedua lampu pada sensor infra merah menyala artinya sensor mendeteksi ada objek di depan. Kondisi jalan yang ditunjukkan Gambar 3 (a) pada sisi selatan terindikasi sebagai lancar sedangkan pada tiga sisi lainnya terindikasikan sebagai sepi, karena tidak sensor yang mendeteksi adanya benda. Sedangkan Gambar 3 (b) adalah kondisi yang menunjukkan indikasi macet di keempat sisi jalan. Kondisi jalan macet ini mengindikasinya semua sensor dapat berfungsi dengan baik mendeteksi adanya benda.




(a) (b) (c)

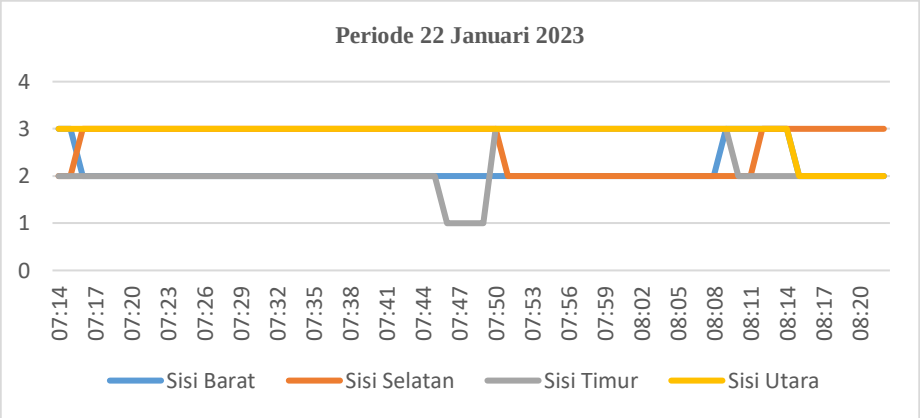
Gambar 3. a) Tampak atas Prototipe monitoring kemacetan lalu lintas, b) Kondisi jalan macet, c) Tampilan Aplikasi Android Monitoring Kemacetan Lalu lintas

Tampilan aplikasi android (lihat Gambar 3**Error! Reference source not found.**(c)), untuk memonitor tingkat kemacetan di keempat sisi jalan, baik secara realtime maupun history data logger. Sisi atas merupakan penyajian informasi secara realtime sedangkan sisi di bawah history merupakan catatan informasi dari data logger yang dapat dipilih oleh pengguna. Aplikasi ini menggunakan koding berbasis block untuk Aplikasi Android yang dibangun menggunakan MIT App Inventor [10].



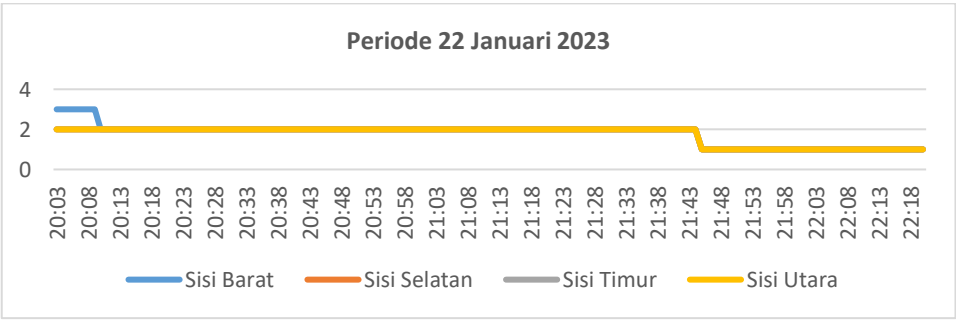

Gambar 4. Grafik Fluktuasi Lalu Lintas Jam 05:50 – 06:14 WIB

Gambar 4 merupakan grafik fluktuasi lalu lintas yang diperoleh dari pengujian pengambilan data sampling. Sumbu Y merupakan indikator kemacetan, untuk angka 1 mengindikasikan jalan sepi, untuk angka 2 mengindikasikan jalan lancar, dan angka 3 mengindikasikan jalan maceet. Sumbu X menunjukkan waktu pengambilan sampling. Pada grafik terlihat terjadi kemacetan di jam 05:55 sampai 05:59, namun setelah jam itu keempat sisi jalan menunjukkan kondisi jalan yang cenderung sepi dan lancar.




Gambar 5. Grafik Fluktuasi Lalu Lintas Jam 07:14 – 08:20 WIB

Sedangkan pada Gambar 5 yang menunjukkan grafik fluktuasi lalu lintas pada jam 07:14 – 08:20 WIB, cenderung menunjukkan kondisi jalan di keempat ruas jalan mengalami kemacetan yang cukup parah. Namun, pada jam 07:44 sampai 07:50 WIB jalan sisi timur menunjukkan kondisi jalan yang sepi Ketika ketiga ruas jalan lainnya cenderung ramai lancer. pada jalan sisi utara cenderung selalu macet sehingga diharapakan pengguna jalan untuk tidak memilih jalan ini untuk rute yang akan ditempuh dan kemacetan itu baru terurai setelah jam 8:17 WIB. Hal ini merupakan Indikasi bahwa jalan tersebut dekat dengan sekolah, karena kerap terjadi kemacetan di pagi hari.




Gambar 6. Grafik Fluktuiasi Lalu Lintas Jam 20:03 – 22:18 WIB

Semua sisi jalan tampak lancar dimulai pada jam 20:08 WIB dan mulai sepi setelah jam 21:43 WIB hal ini terlihat pada Gambar 6. Meskipun di dua gambar grafik sebelumnya sisi utara

yang selalu tampak macet, namun pada jam 20:03 sisi utara terlebih dahulu lancar dibanding sisi barat. Hal ini dapat diindikasikan bahwa terdapat arus balik yang cukup padat, sehingga sisi barat terjadi kemacetan hanya di malam hari.

Pengujian kemampuan sensor inframerah yang digunakan pada prototipe di penelitian dalam mendeteksi benda terjauh adalah 4,5 cm sedangkan pada 4,8 cm, sensor sudah tidak dapat mendeteksi benda di depannya. Jarak yang optimal yang digunakan pada penelitian ini adalah 1 cm.

## KESIMPULAN

Prototipe sistem monitoring kemacetan berbasis IoT, mampu mengetahui kondisi di keempat sisi jalan menggunakan ESP32 yang diintegrasikan dengan dua sensor infra merah di setiap sisi jalan dengan jarak optimal yang digunakan pada penelitian ini adalah 1 cm dan jarak terjauh yang dapat dideteksi adalah 4,5 cm. Prototipe ini juga mampu menyimpan history data log selama pengambilan sampling. Sehingga data log ini dapat dijadikan acuan pengguna dalam menentukan jalan yang akan ditempuh, disamping data realtime pada saat mengambil keputusan.

## DAFTAR PUSTAKA

[1] S. Fatimah, "Kebijakan Pemerintah dalam Mengatasi Kemacetan di Kota Yogyakarta (Studi Penelitian di Jalan Malioboro di JalanTentara Pelajar)," *POPULIKA*, vol. 10, no. 1, pp. 24–41, Jan. 2022, doi: 10.37631/populika.v10i1.473.
[2] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the Internet of Things: A Standardization Perspective," *IEEE Internet Things J.*, vol. 1, no. 3, pp. 265–275, Jun. 2014, doi: 10.1109/JIOT.2014.2323395.
[3] P. A. Rosyady, M. R. Feter, and Z. A. Ikhsan M, "Prototipe Sistem Deteksi Kemacetan Jalan Raya Berbasis Internet Of Things (IoT)," *AVITEC*, vol. 4, no. 2, p. 197, Aug. 2022, doi: 10.28989/avitec.v4i2.1270.
[4] D. S. Riyadi and A. Ramadhan, "Sistem Pemantauan Jarak Jauh Yang Mengintegrasikan Anemometer, Higrometer, Dan Termometer," 2022.
[5] R. A. Firmansyah, T. Suheta, and D. Antoni, "PERANCANGAN ALAT MONITORING DAN PENYIMPAN DATA PADA PANEL HUBUNG TEGANGAN RENDAH DI TRAFO GARDU DISTRIBUSI BERBASIS MIKROKONTROLER," 2015.
[6] S. Siswaya, S. Sunardi, and A. Yudhana, "Analisis Sistem Traffic Light Untuk Optimalisasi dan Antisipasi Kemacetan Lalu Lintas Berbasis Android," *Respati*, vol. 16, no. 3, p. 86, Nov. 2021, doi: 10.35842/jtir.v16i3.423.
[7] A. H. M. Alaidi, I. A. Aljazaery, H. TH. S. Alrikabi, I. N. Mahmood, and F. T. Abed, "Design and Implementation of a Smart Traffic Light Management System Controlled Wirelessly by Arduino," *Int. J. Interact. Mob. Technol. IJIM*, vol. 14, no. 07, p. 32, May 2020, doi: 10.3991/ijim.v14i07.12823.
[8] S. W. Mudjanarko, "PEMANFAATAN INTERNET OF THINGS (IOT) SEBAGAI SOLUSI MANEJEMEN TRANSPORTASI KENDARAAN SEPEDA MOTOR," Open Science Framework, preprint, Dec. 2017. doi: 10.31219/osf.io/6ue4b.
[9] V. Pravalika and C. R. Prasad, "Internet of Things Based Home Monitoring and Device Control Using Esp32," *Int. J. Recent Technol. Eng. IJRTE*, vol. 8, no. 1S4, 2019.
[10] "About Us." http://appinventor.mit.edu/about-us (accessed Jan. 26, 2023).

JREEC
JOURNAL RENEWABLE ENERGY ELECTRONICS AND CONTROL
homepage URL : https://ejurnal.itats.ac.id/jreec

# DETEKSI SERANGAN PING FLOOD PADA SERVER CCTV

*Dani Raisman1, Refdi Andri2, dan Nelly Khairani Daulay3*

*Universitas Bina Insan1,2,3*

**INFORMASI ARTIKEL**

Jurnal JREEC – Volume 03 Nomer 01, Juni 2023

Halaman:
48-58
Tanggal Terbit :
06 Juni 2023

DOI:
10.31284/j.JREEC.2023.v31i.4520

***ABSTRACT***

*The development of information technology, especially computer networks, allows the exchange of information that is easy, fast, and increasingly complex. Computer network security must be considered in order to maintain the validity and integrity of data and information residing in the computer network. The problem that arises in the CCTV control center is that there is no security against the detection of attacks that can occur at any time, for example a ping flood attack. Ping flood itself can be interpreted as a simple denial of service attack in which the attacker floods the victim with "echo request" (ping) packets in the ICMP protocol. To overcome the problems faced by the Lubuklinggau City Police control center in carrying out CCTV server security, the solution offered is to build an Intrusion Detection Server (IDS). IDS itself can read incoming and outgoing data packets automatically which will provide a report (log) to the network administrator. One of the most widely used IDS tools is Snort. Snort has several advantages compared to other IDS software, including source code that is small in size, compatible with many operating systems, fast in detecting network attacks, easy to configure and is open source.*

***Kata kunci:*** *Network security, IDS, Snort*

**EMAIL**

daniraisman1995@gmail.com 1
refdia3@gmail.com 2
nellykhairanilestari@gmail.com 3

**ABSTRAK**

Perkembangan teknologi informasi, khususnya jaringan komputer memungkinkan terjadinya pertukaran informasi yang mudah, cepat, dan semakin kompleks. Keamanan jaringan komputer harus diperhatikan guna menjaga validitas dan integritas data serta informasi yang berada dalam jaringan komputer tersebut. Permasalahan yang timbul di pusat kendali CCTV ini adalah belum adanya pengamanan terhadap pendeteksian serangan yang dapat terjadi kapan saja, sebagai contoh serangan ping flood. Ping flood sendiri dapat diartikan serangan penolakan terhadap layanan sederhana di mana penyerang membanjiri korban dengan paket "echo request" (ping) pada protocol ICMP. Untuk mengatasi permasalahan yang dihadapi oleh pihak pusat kendali Polres Kota Lubuklinggau dalam melakukan keamanan server CCTV tersebut, solusi yang ditawarkan adalah dengan membangun suatu Intrusion Detection Server (IDS). IDS sendiri dapat membaca paket-paket data yang masuk maupun yang keluar secara otomatis yang nantinya akan memberikan sebuah laporan (log) kepada administrator jaringan. Salah satu tools IDS yang banyak digunakan adalah Snort. Snort memiliki beberapa keunggulan dibandingkan software IDS yang lain antara lain source code yang berukuran kecil, kompatibel dengan banyak sistem operasi, cepat dalam mendeteksi serangan jaringan, mudah dikonfigurasi dan bersifat open source.

***Kata kunci:*** *Keamanan Jaringan, IDS, Snort.*

**PENERBIT**

Jurusan Teknik Elektro-ITATS
Alamat:
Jl. Arief Rachman Hakim No.100,Surabaya 60117,
Telp/Fax: 031-5997244

## PENDAHULUAN

Keamanana jaringan merupakana hal yang sangat penting dalam dunia jaringan. Banyak faktor yang dapat mengganggu keamanan dan kestabilan dari suatu koneksi jaringan tersebut. Sistem keamanan jaringan yang baik dapat meminimalisis kerugian yang disebabkan oleh serangan keamanan jaringan[1]. Oleh karena itu, peran sistem keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi merupakan bagian yang penting untuk menjaga validitas dan integritas data serta dapat menjamin ketersediaan layanan bagi penggunanya. Pusat Kendali (Command Center) Polres Lubuklinggau yang selanjutnya disebut Pusat Kendali adalah suatu sistem terpadu berbasis teknologi informasi yang terintegrasi untuk mendukung kegiatan operasional kepolisian dalam rangka pelayanan masyarakat. Salah satu pelayanan terpadu tersebut berupa unit pemantauan layanan CCTV. Seluruh pantauan dari kamera CCTV dilakukan penyimpanan ke dalam sebuah server[2]. Permasalahan yang timbul di pusat kendali CCTV ini adalah belum adanya pengamanan terhadap pendeteksian serangan yang dapat terjadi kapan saja, sebagai contoh serangan ping flood. Ping flood sendiri dapat diartikan serangan penolakan terhadap layanan sederhana di mana penyerang membanjiri korban dengan paket "echo request" (ping) pada protocol ICMP. Dengan tidak adanya pengamanan terhadap kemungkinan serangan yang terjadi, tentunya dapat merugikan pihak dari Polres Kota Lubuklinggau dimana data-data di dalam server tersebut mengalami kerusakan atau bahkan sampai hilang.

Untuk mengatasi permasalahan yang dihadapi oleh pihak pusat kendali Polres Kota Lubuklinggau dalam melakukan keamanan server CCTV tersebut, solusi yang ditawarkan adalah dengan membangun suatu Intrusion Detection Server (IDS). IDS sendiri dapat membaca paket-paket data yang masuk maupun yang keluar secara otomatis yang nantinya akan memberikan sebuah laporan (log) kepada administrator jaringan. Salah satu tools IDS yang banyak digunakan adalah Snort. Snort memiliki beberapa keunggulan dibandingkan software IDS yang lain antara lain source code yang berukuran kecil, kompatibel dengan banyak sistem operasi, cepat dalam mendeteksi serangan jaringan, mudah dikonfigurasi dan bersifat open source.

## TINJAUAN PUSTAKA

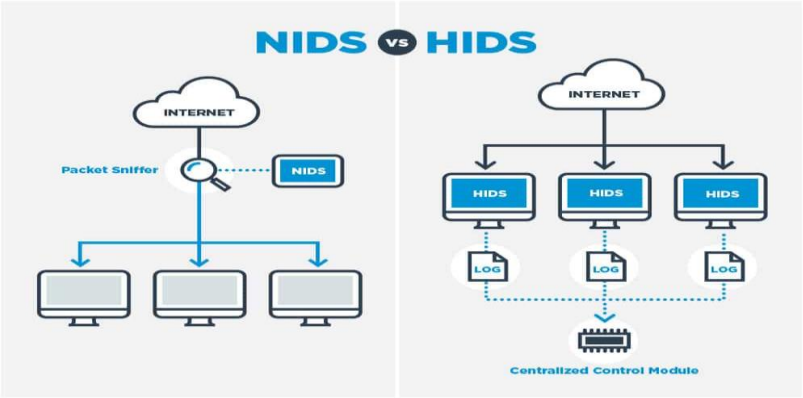
### Intrusion Detection System (IDS)

Intrusion Detection System adalah perangkat lunak atau perangkat keras yang dirancang untuk mendeteksi aktifitas berbahaya baik dalam hal serangan terhadap suatu sistem maupun terhadap suatu jaringan komputer. IDS dapat melakukan inspeksi terhadap lalu lintas jaringan inbound dan outbound dalam suatu jaringan. Ketika menemukan serangan, maka akan memberikan peringatan apakah aktifitas tersebut termasuk berbahaya atau tidak berdasarkan beberapa level, yaitu low, medium, high, dan serious. IDS juga dapat didefinisikan sebagai tool, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer[3]. Aplikasiyang digunakan untuk melakukan penyerangan ke komputer server dalam penelitian ini adalah aplikasi Loic (Low Orbit Ion cannon). Loic (Low Orbit Ion)merupakan sebuah tool atau aplikasi yang berfungsi untuk melumpuhkan server sebuah situs website dengan mengirimkan packet sebanyak mungkin sesuai dengan kemauan si penyerang ke komputer server yang dituju melalui domain atau ip server komputer target. IDS dibagi menjadi 2 (dua) bagian yaitu *Network-based IDS* (NIDS) dan *Host-based IDS (HIDS)*

### *Network-based IDS* (NIDS)

Berfungsi untuk memantau dan memonitor semua lalu lintas jaringan pada keseluruhan jaringan, NIDS akan menangkap semua lalu lintas jaringan dan mengirimkan *copy* dari lalu lintas yang ditangkap dan mengirimkan ke IDS. NIDS biasanya diletakkan di dalam segmen jaringan di

mana *server* berada atau di pintu masuk jaringan. Contoh IDS yaitu *Snort*. Gambar 2.1 menyajikan ilustrasi NIDS dan HIDS.




**Gambar 2.1** Ilustrasi NIDS dan HIDS

***Host-based IDS (HIDS)***

Berfungsi memantau dan menganalisis lalu lintas jaringan yang masuk dan keluar dari *host*. Perbedaan utama HIDS dengan NIDS adalah NIDS memonitor seluruh segmen jaringan, sedangkan HIDS hanya memonitor pada *host* tertentu, biasanya diletakkan di *server-server* kritis di jaringan seperti *firewall* dan *web server*. HIDS juga menangkap lalu lintas jaringan seperti *snapshot* dan dibandingkan dengan *snapshot* sebelummnya, jika terdapat perbedaan maka akan mengirimkan alert kepada administrator.

***Snort***

Snort merupakan sebuah perangkat lunak yang berfungsi untuk mengamati aktifitas dalam suatu jaringan komputer. Komponen pada Snort terdiri dari beberapa bagian yaitu:

a. *Packet Decoder*
   Berfungsi untuk mengekstrak paket dari jaringan dalam bentuk file berformat 'tcpdump' dan mengirimkan paket ke *preprocessor*.
b. *Preprocessor*
   Berfungsi untuk memodifikasi paket yang rusak menggunakan beberapa operasi dan kemudian mengirimkan ulang ke *Detection Engine*.
c. *Detection Engine*
   Berfungsi untuk mendeteksi ancaman aktivitas yang ada dalam paket dengan menggunakan *snort rules*.
d. *Logging and Alerting System*
   Berfungsi untuk menghasilkan alarm atau log aktivitas intrusi yang terdeteksi oleh *Detection Engine*.
e. *Output Modules*
   Berfungsi untuk menyimpan output yang dihasilkan oleh *Logging and Alerting System*.
   Adapun dalam mengoperasikan Snort ada beberapa cara, antara lain:
   1) *Sniffer mode*: Pada mode ini, *Snort* akan menangkap semua paket pada jaringan tertentu.
   2) *Packet Logger Mode*: Pada mode ini, *Snort* akan menangkap semua paket yang melintas, dan menyimpan di *storage*.
   3) *Network Intrusion Detection Mode*: Pada mode ini, *Snort* akan menjalan *file* konfigurasi yang sudah diatur pada *file* 'snort.conf'.

**Serangan Pada Jaringan Komputer**

Ada berbagai macam serangan pada jaringan komputer, beberpa diantara di jelaskan sebagai berikut**:**

**LAND Attack**

Salah satu serangan terhadap suatu server yang terhubung dalam suatu jaringan untuk menghentikan layanan, sehingga terjadi gangguan terhadap layanan atau jaringan computer. Tipe serangan semacam ini disebut sebagai Denial of Service (DoS) attack[4]. LAND attack dikategorikan sebagai serangan SYN (SYN attack) karena menggunakan packet SYN (synchronization) pada waktu melakukan 3-way handshake untuk membentuk suatu hubungan berbasis TCP/IP.

**Ping of Death**

Ping of Death merupakan suatu serangan (Denial of Service) DoS yang memanfaatkan fitur yang ada di TCP/IP yaitu packet fragmentation atau pemecahan paket. Penyerang dapat mengirimkan berbagai paket ICMP (digunakan untuk melakukan ping) yang terfragmentasisehingga waktu paket-paket tersebut disatukan kembali, maka ukuran paket seluruhnya melebihi batas 65536 byte.

**Teardrop**

Teardrop attack adalah suatu serangan bertipe Denial of Service (DoS) terhadap suatu server/komputer yang memanfaatkan fitur yang ada di TCP/IP yaitu packet fragmentation atau pemecahan paket, dan kelemahan yang ada di TCP/IP pada waktu paket-paket yang terfragmentasi tersebut disatukan kembali[5]. Dalam suatu pengiriman data dari satu komputer ke komputer yang lain melalui jaringan berbasis TCP/IP, maka data tersebut akan dipecah-pecah menjadi beberapa paket yang lebih kecil di komputer asal, dan paket-paket tersebut dikirim dan kemudian disatukan kembali di komputer tujuan. Server bisa diproteksi dari tipe serangan teardrop ini dengan paket filtering melalui firewall yang sudah dikonfigurasi untuk memantau dan memblokir paket-paket yang berbahaya seperti ini.

**Half-Open Connection**

Dalam serangan half-open connection, penyerang mengirimkan ke server yang hendak diserang banyak paket SYN yang telah dispoof atau direkayasa sehingga alamat asal (source address) menjadi tidak valid[6]. Tipe serangan half-open connection atau SYN attack ini dapat dicegah dengan paket filtering dan firewall, sehingga paket-paket SYN yang invalid tersebut dapat diblokir oleh firewall sebelum membanjiri server.

**UDP Bomb Attack**

Untuk melakukan serangan UDP Bomb terhadap suatu server, seorang penyerang mengirim sebuah paket UDP (User Datagram Protocol) yang telah dispoof atau direkayasa sehingga berisikan nilai-nilai yang tidak valid di field-field tertentu[7]. Jika server yang tidak terproteksi masih menggunakan sistem operasi (operating system) lama yang tidak dapat menangani paketpaket UDP yang tidak valid ini, maka server akan langsung crash.

## METODE

**Metode Pengumpulan data**

Untuk mendapatkan data yang akurat maka dalam penyusunan proposal skirpsi ini penulis mengunakan beberapa metode pengumpulan data diantaranya adalah sebagai berikit ini :

a. Observasi

   Merupakan teknik atau pendekatan untuk mendapatkan data primer dengan mengamati langsung objek datanya sehingga data dapat diproleh secara orisinil pada saat terjadinya dan mencatatkan hasil observasi tersebut. Dengan melakukan observasi langsung untuk mencari informasi data baik alat dan bahan serta segala sesuatu yang digunakan dalam penelitian ini.

b. Wawancara

   Wawancara digunakan sebagai teknik pengumpulan data pada penelitian ini. Selain itu penulis juga melakukan wawancara yang menyangkut masalah potensi serangan terhadap server CCTV di *command center* Polres Kota Lubuklinggau.

c. Studi Literatur
Menggunakan metode pengumpulan data Literatur yaitu dengan mencari referensi dari buku, majalah, jurnal, artikel, internet, dan sumber lainnya yang berkaitan dengan judul yang diambil, kemudian dirangkum untuk disusun dan di sempurnakan

**Metode Pengembangan Sistem**

Dalam penelitian ini penulis menggunakan metode *Live Forensic* untuk membangun sistem deteksi serangan server CCTV di command center Polres Lubuklinggau[8]. Berikut merupakan langkah-langkah pengembangan perangkat tersebut:

a. *Preparation and collection*
Pada tahapan ini dilakukan pengumpulan data, analisis sistem berjalan, dan analisis sistem yang akan dirancang.
b. *Examination*
Pada tahapan ini dilakukan inspeksi terhadap perangkat keras dan perangkat lunak yang digunakan.
c. *Analysis*
Pada tahap ini dilakukan analisis terhadap hasil skenario penyerangan terhadap sistem. Scenario dilakukan dengan melakukan serangan pada protocol ICMP yang ada di komputer server CCTV.
c. *Log*
Setelah dilakukan analisis, maka dilakukan pencatatan (log) terhadap hasil analisis dari deteksi serangan yang terjadi[9]. Pada tahapan ini akan diketahui apakah Snort yang digunakan untuk mendeteksi serangan ping flood efektif atau tidak.

**Metode Pengujian Sistem**

Pengujian dilakukan dengan menggunakan metode eksperimen yang dimaksudkan apakah sistem Snort dapat mendeteksi serangan *ping flood* dengan baik[10]. Pengujian dilakukan dengan menggunakan *ping flood* yang akan dilakukan oleh komputer *client*. Tabel 3.3 menyajikan perancangan pengujian sistem.

**Tabel 3.3** Perancangan Pengujian

| No | Komponen Pengujian | Proses Pengujian | Hasil Pengujian |
|---|---|---|---|
| 1 | Komputer server | Kinerja *Snort* pada IDS. | Snort dapat mendeteksi serangan yang dilakukan *client.* |
| 2 | Komputer Client | Melakukan *ping flood* ke komputer *server*. | Paket-paket data yang berisi serangan *ping flood*. |

**Rancangan Sistem**

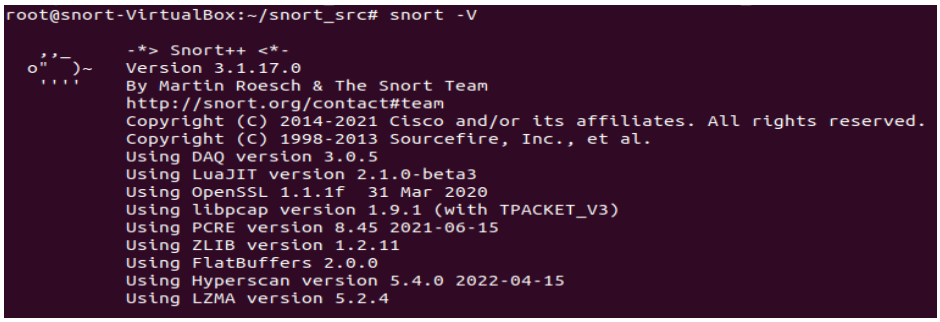
Rancangan sistem dimaksudkan untuk membangun eksperimen terhadap model serangan ping flood yang akan dideteksi[11]. Rancangan eksperimen ini dibagi menjadi 2 bagian, antara lain perancangan perangkat keras dan perancangan perangkat lunak. Dalam proses perancangan perangkat keras, eksperimen ini dibangun dengan menggunakan 2 PC / laptop. PC1 digunakan sebagai server yang diinstalasi Snort dan PC2 sebagai client yang bertindak sebagai attacker. Gambar 3.4 menyajikan rancangan perangkat keras yang akan dibangun, dapat dilihat dibawah ini :


**Gambar 3.4** Rancangan Topologi Eksperimen

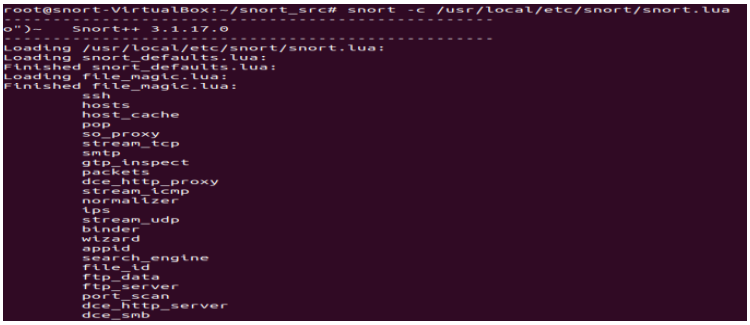
## HASIL DAN PEMBAHASAN

### Pembahasan Data I

Hasil Instalasi Snort, Untuk tahap pertama dari adalah hasil instalasi snort 3 dapat ditunjukkan pada gambar 4.1, dan pengujian snort berjalan dengan baik ditunjukan pada gambar 4.2.



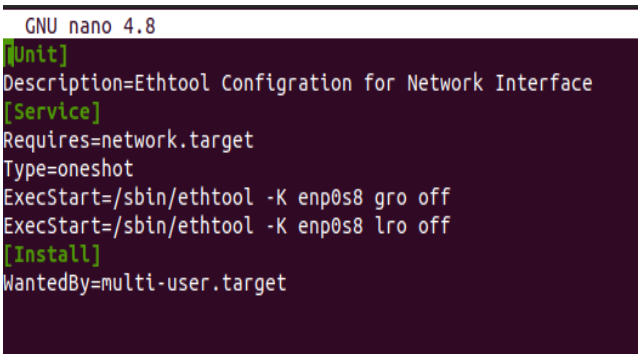

**Gambar 4.1** Hasil Instalasi Snort



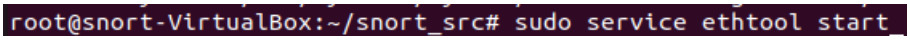

**Gambar 4.2** Pengujian Hasil Instalasi

Gambar 4.3 dan gambar 4.4 menunjukkan konfigurasi perangkat ethernet yang akan di monitor atau diawasi oleh snort dan mengaktifkannya[12].

### Pembahasan Data II




**Gambar 4.3** Pengaturan Perangkat Ethernet




**Gambar 4.4** Aktifasi Perangkat Ethernet

Gambar 4.5 menunjukkan direktori untuk menyimpan *rule* snort, *rule* ini digunakan untuk menyimpan perintah pada snort dalam mendeteksi serangan yang sudah didefinisikan.

```
sudo mkdir /usr/local/etc/rules
sudo mkdir /usr/local/etc/so_rules/
sudo mkdir /usr/local/etc/lists/

sudo touch /usr/local/etc/rules/local.rules
sudo touch /usr/local/etc/lists/default.blocklist

sudo mkdir /var/log/snort
```

**Gambar 4.5** Direktori Pengaturan Snort

Gambar 4.6 adalah *rule* atau aturan yang penulis buat untuk mendeteksi serangan *ping flood,* serangan *ping flood* menggunakan paket data protokol ICMP yang dikirimkan secara *masive* sehingga server akan mengalami kelebihan paket data yang diterima sehingga menyebabkan pengguna lain yang mengakses server tersebut menjadi terhambat[13].

```
 GNU nano 4.8                                  /usr/local/etc/rules/local.rules
alert icmp any any -> any any ( msg:"Mendeteksi lalulintas Data ICMP  "; sid:10000001; metadata:policy security-ips alert; )
```

**Gambar 4.6** Rule Snort Deteksi Ping Flood

*Rule* atau aturan yang penulis buat untuk mendeteksi *ping flood* adalah dengan mendeteksi paket data ICMP yang berlebihan, dan melewati ethernet yang sudah dimasukkan dalam pengaturan snort untuk diawasi[14].

**Pembahasan Data III**

Gambar 4.7 dan 4.8 menunjukkan penggunaan *rule* untuk mendeteksi serangan *ping flood* dan hasil deteksi serangan *ping flood* pada server[15].

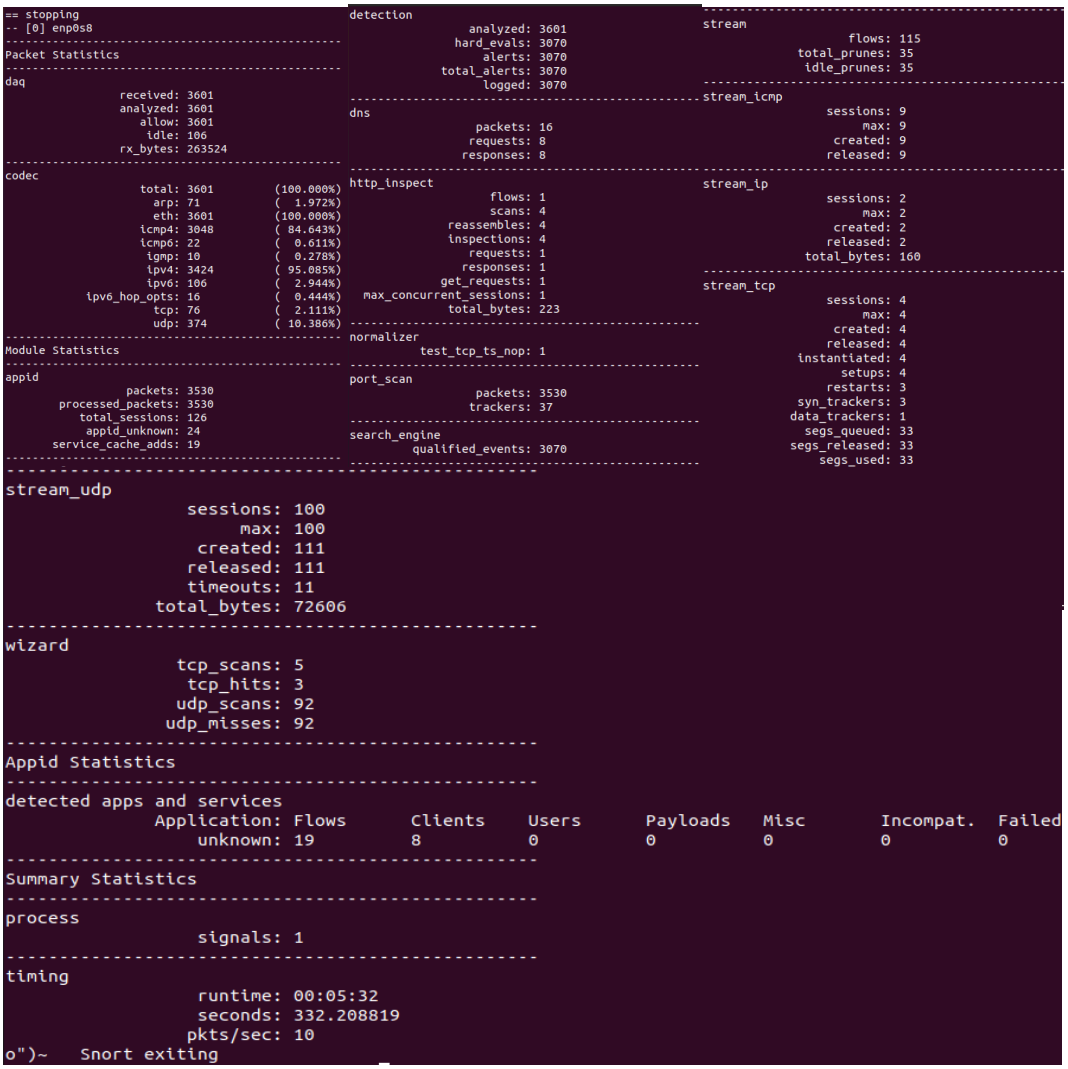
```
root@snort-VirtualBox:~/snort_src# sudo snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/rules/local.rules \
> -i enp0s8 -A alert_fast -s 65535 -k none
```

**Gambar 4.7** Penerapan *rule* snort untuk mendeteksi *ping flood* secara *real time*

```
04/15-09:16:12.238565 [**] [1:10000001:0] "Mendeteksi lalulintas Data ICMP  " [**] [Priority: 0] {ICMP} 192.168.88.246 -> 192.168.88.248
04/15-09:16:12.238591 [**] [1:10000001:0] "Mendeteksi lalulintas Data ICMP  " [**] [Priority: 0] {ICMP} 192.168.88.248 -> 192.168.88.246
04/15-09:16:12.270914 [**] [1:10000001:0] "Mendeteksi lalulintas Data ICMP  " [**] [Priority: 0] {ICMP} 192.168.88.246 -> 192.168.88.248
04/15-09:16:12.270935 [**] [1:10000001:0] "Mendeteksi lalulintas Data ICMP  " [**] [Priority: 0] {ICMP} 192.168.88.248 -> 192.168.88.246
04/15-09:16:12.303216 [**] [1:10000001:0] "Mendeteksi lalulintas Data ICMP  " [**] [Priority: 0] {ICMP} 192.168.88.246 -> 192.168.88.248
04/15-09:16:12.303236 [**] [1:10000001:0] "Mendeteksi lalulintas Data ICMP  " [**] [Priority: 0] {ICMP} 192.168.88.248 -> 192.168.88.246
04/15-09:16:12.335161 [**] [1:10000001:0] "Mendeteksi lalulintas Data ICMP  " [**] [Priority: 0] {ICMP} 192.168.88.246 -> 192.168.88.248
04/15-09:16:12.335181 [**] [1:10000001:0] "Mendeteksi lalulintas Data ICMP  " [**] [Priority: 0] {ICMP} 192.168.88.248 -> 192.168.88.246
04/15-09:16:12.367275 [**] [1:10000001:0] "Mendeteksi lalulintas Data ICMP  " [**] [Priority: 0] {ICMP} 192.168.88.246 -> 192.168.88.248
04/15-09:16:12.367298 [**] [1:10000001:0] "Mendeteksi lalulintas Data ICMP  " [**] [Priority: 0] {ICMP} 192.168.88.248 -> 192.168.88.246
04/15-09:16:12.398650 [**] [1:10000001:0] "Mendeteksi lalulintas Data ICMP  " [**] [Priority: 0] {ICMP} 192.168.88.246 -> 192.168.88.248
```

**Gambar 4. 8** Hasil deteksi serangan *ping flood* secara *real time*

Gambar 4.9 menunjukkan statistik hasil deteksi *ping flood* secara *real time* menggunakan snort. Dari gambar 4.9 tersebut dapat dilihat ip address dari computer penyerang yaitu 192.168.88.246 dengan serangan ping flood yang membanjiri lalu lintas data di protocol ICMP. Dampak dari serangan ini akan meningkatnya penggunaan resource sumber daya computer server seperti CPU hingga 100 % bahkan overload[16].




**Gambar 4.9** Hasil Deteksi Serangan Ping Flood

Dari pengujian yang telah dilakukan maka dapat ditarik kesimpulan sistem deteksi serangan ping flood dapat mendeteksi serangan tersebut secara real time[17].

## KESIMPULAN

Hasil dari penelitian ini berguna Untuk mengatasi permasalahan yang dihadapi oleh pihak pusat kendali Polres Kota Lubuklinggau dalam melakukan keamanan server CCTV tersebut, selain itu juga untuk membuat sistem keamanan jaringan dalam mengatasi serangan ping flood di server CCTV Polres Kota Lubuklinggau dapat menggunakan Snort pada IDS. Solusi yang ditawarkan adalah dengan membangun suatu *Intrusion Detection Server* (IDS). IDS sendiri dapat membaca paket-paket data yang masuk maupun yang keluar secara otomatis yang nantinya akan memberikan sebuah laporan (log) kepada administrator jaringan. Salah satu tools IDS yang banyak digunakan adalah *Snort*. *Snort* memiliki beberapa keunggulan dibandingkan software IDS yang lain antara lain *source code* yang berukuran kecil, kompatibel dengan banyak sistem operasi, cepat dalam mendeteksi serangan jaringan, mudah dikonfigurasi dan bersifat *open source*.

**DAFTAR PUSTAKA**

[1] A. H. Hambali and S. Nurmiati, "Implementasi Intrusion Detection System (IDS) Pada Keamanan PC Server Terhadap Serangan Flooding Data," *Sainstech J. Penelit. dan Pengkaj. Sains dan Teknol.*, vol. 28, no. 1, pp. 35–43, 2018, doi: 10.37277/stch.v28i1.267.

[2] P. Panggabean, "Analisis Network Security Snort Metode Intrusion Detection System Untuk Optimasi Keamanan Jaringan Komputer," *Jursima*, vol. 6, no. 1, p. 1, 2018, doi: 10.47024/js.v6i1.107.

[3] S. M. Othman, F. Mutaher Ba-Alwi, N. T. Alsohybe, and A. T. Zahary, "Survey on Intrusion Detection System Types," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 4, pp. 444–462, 2018, [Online]. Available: https://www.researchgate.net/publication/329363322

[4] B. Wijaya and A. Pratama, "Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (Ids) Berbasis Snort," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 1, pp. 97–101, 2020, doi: 10.32736/sisfokom.v9i1.770.

[5] I. P. A. E. Pratama and N. K. M. Handayani, "Implementasi IDS Menggunakan Snort Pada Sistem Operasi Ubuntu," *J. Mantik Penusa*, vol. 3, no. 1, pp. 176–181, 2019.

[6] S. Khadafi, Y. D. Pratiwi, and E. Alfianto, "Keamanan Ftp Server Berbasiskan Ids Dan Ips Menggunakan Sistem Operasi Linux Ubuntu," *Netw. Eng. Res. Oper.*, vol. 6, no. 1, p. 11, 2021, doi: 10.21107/nero.v6i1.190.

[7] I. G. N. W. Arsa, "Arsitektur Konsolidasi Server dengan Virtualisasi untuk Penyedia Layanan Infrastruktur Cloud," *J. Sist. dan Inform.*, vol. 14, no. 1, pp. 35–40, 2019, doi: 10.30864/jsi.v14i1.240.

[8] O. A. Astra and Y. Mardiana, "Rancang Bangun dan Analisa Pengendali CCTV Berbasis Arduino Menggunakan Smartphone Android," *J. Media Infotama*, vol. 14, no. 1, 2018, doi: 10.37676/jmi.v14i1.470.

[9] D. V. Sandi and M. Arrofiq, "Implementasi Analisis NIDS Berbasis Snort Dengan Metode Fuzy Untuk Mengatasi Serangan LoRaWAN," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 3, pp. 685–696, 2018, doi: 10.29207/resti.v2i3.504.

[10] F. Antony and R. Gustriansyah, "Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 21, no. 1, pp. 43–52, 2021, doi: 10.30812/matrik.v21i1.1078.

[11] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Perancangan Digital Forensik pada Aplikasi Twitter Menggunakan Metode Live Forensics," *Semin. Nas. Inform. 2008 (semnasIF 2008)*, vol. 2018, no. November, pp. 86–91, 2018.

[12] D. Santoso, A. Noertjahyana, and J. Andjarwirawan, "Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS," *J. Infra*, vol. 10, no. 1, pp. 1–6, 2022, [Online]. Available: https://publication.petra.ac.id/index.php/teknik-informatika/article/view/12033

[13] I. Riadi, S. Sunardi, and M. E. Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," *J. Tek. Elektro*, vol. 10, no. 1, pp. 18–22, 2018, doi: 10.15294/jte.v10i1.14070.

[14] R. Suwanto, I. Ruslianto, and M. Diponegoro, "Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IPTable Pada Monitoring Jaringan Lokal Berbasis Website," *J. Komput. dan Apl.*, vol. 07, no. 1, pp. 97–107, 2019.

[15] I. K. K. A. Marta, I. N. B. Hartawan, and I. K. S. Satwika, "Analisis Sistem Monitoring Keamanan Server Dengan Sms Alert Berbasis Snort," *Inser. Inf. Syst. Emerg. Technol. J.*, vol. 1, no. 1, p. 25, 2020, doi: 10.23887/insert.v1i1.25874.

[16] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *Aiti*, vol. 17, no. 2, pp. 143–158, 2021, doi: 10.24246/aiti.v17i2.143-158.

[17] Soni, Y. Prayudi, and B. Sugiantoro, "Teknik Akuisisi Virtualisasi Server Menggunakan Metode Live Forensic," *Teknomatika*, vol. 9, no. 2, 2017.

JREEC
JOURNAL RENEWABLE ENERGY ELECTRONICS AND CONTROL
homepage URL : https://ejurnal.itats.ac.id/jreec

# SISTEM DETEKSI KEAMANAN JARINGAN PADA SERVER DAPODIK DI SMPN I MUARA KELINGI TERHADAP SERANGAN SNIFFING

*Resha Purnama Sari1, Asep Toyib Hidayat2, Phito Prima Sanjaya3, Anisya Apriliana4*

*Universitas Bina Insan1,2,3,4*

**INFORMASI ARTIKEL**

Jurnal JREEC – Volume 03 Nomer 01, Juni 2023

Halaman:
57-65
Tanggal Terbit :
06 Juni 2023

DOI:
10.31284/j.JREEC.2023.v31i.4552

**EMAIL**

1902010007@mhs.univbinainsan.ac.id 1
Asep_toyib_hidayat@univbinainsan.ac.id 2
phitosanjaya12@gmail.com 3
anisyaapriliana24@gmail.com 4

**PENERBIT**

Jurusan Teknik Elektro-ITATS
Alamat:
Jl. Arief Rachman Hakim No.100,Surabaya 60117,
Telp/Fax: 031-5997244



***ABSTRACT***

*Information technology (IT) has been applied to various sectors, including industry, government, education and health. However, technological sophistication is also accompanied by threats in terms of data security. For this reason, a system is needed that can secure the data, where attacks on data often occur from networks connected to the internet. The world of education today is also very dependent on technological sophistication, especially in data storage. One that utilizes this technology is SMPN I Muara Kelingi. The problem currently faced is the lack of a data security system on the Dapodik Server at SMPN I Muara Kelingi. The attack that can attack the network is in the form of a sniffing attack. The purpose of making this system is so that the data or information contained in the system cannot be accessed by unauthorized persons and to prevent damage to the system. By using the Security Policy Development Life Cycle (SPDLC) and using Snort as a tool to detect packet sniffing attacks, the school can quickly detect attacks that occur on the school Dapodik Server.*

***Kata kunci:*** *Network Security, SPDLC, Snort, Dapodik Server, Sniffing.*

**ABSTRAK**

Teknologi informasi (IT) telah diterapkan pada berbagai sektor, baik industri, pemerintahan, pendidikan dan kesehatan. Namun kecanggihan teknologi juga di sertai dengan ancama-ancaman dari segi keamanan datanya. Untuk itu diperlukan sebuah sistem yang dapat mengamankan data tersebut, dimana penyerangan terhadap data sering terjadi dari jaringan yang terhubung ke internet. Dunia pendidikan saat ini juga sangat bergantung dengan kecanggihan teknologi terutama dalam penyimpanan data. Salah satu yang memanfaatkan teknolgi ini adalah SMPN I Muara Kelingi. Permasalahan yang dihadapi saat ini adalah kurangnya sistem pengamanan data pada Server Dapodik SMPN I Muara Kelingi. Serangan yang dapat menyerang jaringan tersebut berupa serangan Sniffing. Tujuannya dibuatnya sistem ini adalah agar data atau informasi yang ada dalam sistem tidak dapat diakses oleh orang yang tidak berkepentingan serta untuk mencegah tindakan pengerusakan terhadap sistem tersebut. Dengan menggunakan Security Policy Development Life Cycle (SPDLC) serta menggunakan Snort sebagai alat untuk mendeteksi serangan packet sniffing maka pihak sekolah dapat mendeteksi dengan cepat serangan yang terjadi pada Server Dapodik sekolah.

***Kata kunci:*** *Keamanan Jaringan, SPDLC, Snort, Server Dapodik, Sniffing..*

## PENDAHULUAN

Seiring dengan kemajuan teknologi informasi (IT) yang telah banyak diterapan oleh hampir semua kalangan munculah permasalahan tentang keamanan dari sistem IT, agar data atau informasi yang ada didalam sistem tidak bisa diakses oelh orang yang tidak berkepentingan, dan bagai mana agar sistem tersebut terhindar dari tindakan pengerusakan[1]. Berbagai Isu keamanan jaringan saat ini menjadi sangat penting dan patut untuk diperhatikan. Sebuah jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para hacker, baik jaringan wired LAN maupun wireless LAN. Pada saat proses pengiriman data akan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menyadap atau mengubah data tersebut. SMPN I Muara Kelingi adalah sebuah sekolah menengah pertama yang berada di ibukota Kecamatan Muara Kelingi, dalam pendataan pokok sekolah, SMPN I Muara Kelingi harus menggunakan layanan dapodik. Layanan Dapodik adalah suatu sistem pendataan yang dikelola oleh Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi yang memuat data sekolah, peserta didik, pendidik dan tenaga kependidikan, dan substansi pendidikan yang datanya bersumber dari sekolah, tentunya sebagai data pokok sekolah yang dilaporkan ada berbagai data yang bersifat rahasia yang harus diamankan.

Permasalahan yang timbul di layanan Dapodik SMPN I Muara Kelingi adalah belum adanya pengamanan terhadap serangan serta penyusupan yang kapanpun dapat terjadi dalam jaringan dan dapat merugikan pihak sekolah, sebagai contoh serangan Sniffing[2]. Serangan Sniffing adalah teknik pemantauan setiap paket yang melintasi jaringan, dan bagian dari perangkat lunak atau perangkat keras yang memonitor semua lalu lintas jaringan. Potensi bahaya packet sniffing adalah hilangnya prifasi, dan tercurinya informasi penting dan rahasia yang dimiliki oleh user. Untuk mengatasi permasalah tersebut maka dibutuhkan sebuah sistem yang dapat mendeteksi serangan packet sniffing pada jaringan layanan Dapodik SMPN I Muara Kelingi sebagai pencegahan dari serangan pihak yang tidak bertanggung jawab serta pengamanan jaringan berbasis IDS (Intrusion Detection System) menggunakan Snort sebagai alat untuk mendeteksi serangan packet sniffing tersebut. Tujuannya dibuatnya sistem keamanan ini adalah upaya pengamanan server dapodik terhadap serangan sniffing dari pihak yang tidak bertanggung jawab dan Mempermudah pihak SMPN I Muara Kelingi untuk mendeteksi serangan *sniffing* pada jaringan layanan dapodik.

## TINJAUAN PUSTAKA

### Intrusion Detection System (IDS)

Intrusion Detection System adalah perangkat lunak atau perangkat keras yang dirancang untuk mendeteksi aktifitas berbahaya baik dalam hal serangan terhadap suatu sistem maupun terhadap suatu jaringan komputer. IDS dapat melakukan inspeksi terhadap lalu lintas jaringan inbound dan outbound dalam suatu jaringan[3]. Ketika menemukan serangan, maka akan memberikan peringatan apakah aktifitas tersebut termasuk berbahaya atau tidak berdasarkan beberapa level, yaitu low, medium, high, dan serious. IDS juga dapat didefinisikan sebagai tool, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer. Aplikasiyang digunakan untuk melakukan penyerangan ke komputer server dalam penelitian ini adalah aplikasi Loic (Low Orbit Ion cannon). Loic (Low Orbit Ion)merupakan sebuah tool atau aplikasi yang berfungsi untuk melumpuhkan server sebuah situs website dengan mengirimkan packet sebanyak mungkin sesuai dengan kemauan si penyerang ke komputer server yang dituju melalui domain atau ip server komputer target.

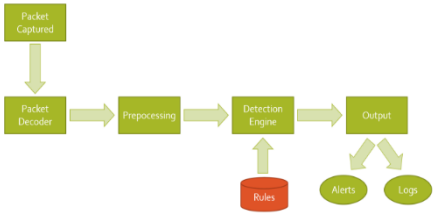
### *Snort*

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu dapat menganalisis lalu lintas real-time, hal ini dapat mendeteksi berbagai jenis serangan. Snort bukanlah sebatas protocol analisis atau sistem pendeteksi penyusupan (Intrusion Detection System) IDS, melainkan sedikit gabungan diantara keduanya, dan bisa sangat berguna dalam merespons insiden-insiden peyerangan terhadap hosthost jaringan[4]. Fitur Snort dapat menjadi penolong administrator sistem dan jaringan, dimana mampu memperingatkan kita atas penyusup yang berpeluang berbahaya. Snort adalah perangkat Intrusion Detection System, bukan Intrusion Prevention System yang dapat

mecegah adanya suatu serangan. Snort hanya dapat memberikan suatu peringatan tentang adanya sebuah serangan terhadap suatu sistem, sehingga untuk dapat melakukan pencegahan terhadap sebuah serangan harus dilakukan[5]. Snort merupakan sebuah perangkat lunak yang berfungsi untuk mengamati aktifitas dalam suatu jaringan komputer. Komponen pada Snort terdiri dari beberapa bagian yaitu:

1. *Packet Decoder*
   Berfungsi untuk mengekstrak paket dari jaringan dalam bentuk file berformat 'tcpdump' dan mengirimkan paket ke preprocessor.
2. *Preprocessor*
   Berfungsi untuk memodifikasi paket yang rusak menggunakan beberapa operasi dan kemudian mengirimkan ulang ke Detection Engine.
3. *Detection Engine*
   Berfungsi untuk mendeteksi ancaman aktivitas yang ada dalam paket dengan menggunakan snort rules.
4. *Logging and Alerting System*
   Berfungsi untuk menghasilkan alarm atau log aktivitas intrusi yang terdeteksi oleh Detection Engine.
5. *Output Modules*
   Berfungsi untuk menyimpan output yang dihasilkan oleh *Logging and Alerting System*.
   Ada beberapa mode yang dilakukan oleh Snort antara lain:
   1) *Packet Sniffer* – Membaca paket dari network kemudian menampilkan dalam bentuk *continuous stream di console screen*
   2) *Packet Logger* – Mencatat semua paket yang lewat di jaringan untuk dianalisa di kemudian hari
   3) *Intrusion Detection Mode* – Pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini di perlukan *setup* dari berbagai *rules* / aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.

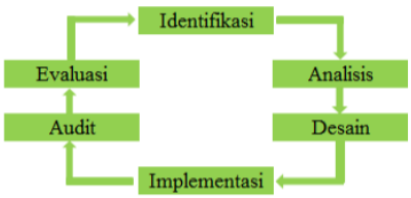
   Alur *IDS* menggunakan *SNORT* dapat dilihat pada gamabr 1 dibawa ini:




Gambar 1. Alur IDS Menggunakan SNORT

**SPDLC (*Security Policy Development Life Cycle)***

*Security Policy Development Life Cycle* (SPDLC) adalah sebuah metode pengembangan sistem yang berfokus pada keamanan jaringan. Gambaran dari metode Security Policy Development Life Cycle dapat dilihat pada gambar 2 dibawah ini :




Gambar 2. Metode *Security Policy Development Life Cycle*

Berikut penjelasan dari tahap-tahap yang dilakukan dalam metode *Security Policy Development Life Cycle* (SPDLC) :

a. Identifikasi
   Tahap awal ini dilakukan untuk menemukan berbagai macam masalah keamanan yang dihadapi oleh jaringan pada saat ini dan bagaimana sistem yang sedang berjalan di perusahaan
b. Analisis
   Dari data yang didapatkan pada tahap identifikasi, dilakukan proses analisis kebutuhan user.
c. Desain
   Tahap desain ini akan membuat suatu gambar rancangan topologi sistem keamanan yang akan dibangun, alur sistem autentikasi serta menjelaskan kebutuhan sistem baik software maupun hardware.
d. Implementasi
   Pada tahap ini dilakukan penerapan dari hasil perancangan yang telah dilakukan pada tahap sebelumnya. Namun, karena keterbatasan izin dari perusahaan dalam melakukan implementasi, hasil perancangan akan disimulasikan dalam jaringan yang lebih kecil[6]. Dimulai dengan instalasi perangkat dan mengkonfigurasi software dan hardware yang diperlukan.
e. Audit
   Pada tahap ini sistem yang disimulasikan akan diuji secara sistematis untuk memastikan bahwa sistem keamanan yang diterapkan sudah sesuai dengan tujuan awal. Tahap ini dilakukan dengan skenario testing.
f. Evaluasi
   Pada tahap ini dilakukan evaluasi hasil dari testing yang telah dilakukan, sejauh mana tingkat efektifitas dari teknologi keamanan yang dibangun, dan membandingkan dengan tujuan awal serta kondisi ideal yang diharapkan[7].

## METODE

### 3.1 Metode Pengumpulan Data

Untuk mendapatkan data yang akurat maka dalam penyusunan proposal skirpsi ini penulis mengunakan beberapa metode pengumpulan data diantaranya adalah sebagai berikit ini :

a. Observasi
   Merupakan teknik atau pendekatan untuk mendapatkan data primer dengan mengamati langsung objek datanya sehingga data dapat diproleh secara orisinil pada saat terjadinya dan mencatatkan hasil observasi tersebut. Dengan melakukan observasi langsung untuk mencari informasi data baik alat dan bahan serta segala sesuatu yang digunakan dalam penelitian ini.
b. Wawancara
   Wawancara digunakan sebagai teknik pengumpulan data pada penelitian ini. Selain itu penulis juga melakukan wawancara yang menyangkut masalah potensi serangan terhadap server SMPN I Muara Kelingi berkaitan dengan server dapotik.
c. Studi Literatur
   Menggunakan metode pengumpulan data Literatur yaitu dengan mencari referensi dari buku, majalah, jurnal, artikel, internet, dan sumber lainnya yang berkaitan dengan judul yang diambil, kemudian dirangkum untuk disusun dan di sempurnakan.

### 3.2 Metode Pengembangan Sistem

Dalam Metodologi yang digunakan dalam penelitian ini adalah *Security Policy Development Life Cycle* (SPDLC). Berikut penjelasan tahap-tahap yang dilakukan dalam penelitian ini:

a. Identifikasi
Tahap awal ini dilakukan untuk menemukan berbagai macam masalah keamanan yang dihadapi oleh jaringan pada saat ini dan bagaimana sistem yang sedang berjalan di perusahaan

b. Analisis
Dari data yang didapatkan pada tahap identifikasi, dilakukan proses analisis kebutuhan user.

c. Desain
Tahap desain ini akan membuat suatu gambar rancangan topologi sistem keamanan yang akan dibangun, alur sistem autentikasi serta menjelaskan kebutuhan sistem baik *software* maupun *hardware*.

d. Implementasi
Pada tahap ini dilakukan penerapan dari hasil perancangan yang telah dilakukan pada tahap sebelumnya. Namun, karena keterbatasan izin dari perusahaan dalam melakukan implementasi, hasil perancangan akan disimulasikan dalam jaringan yang lebih kecil[8]. Dimulai dengan instalasi perangkat dan mengkonfigurasi *softwar*e dan *hardware* yang diperlukan.

e. Audit
Pada tahap ini sistem yang disimulasikan akan diuji secara sistematis untuk memastikan bahwa sistem keamanan yang diterapkan sudah sesuai dengan tujuan awal. Tahap ini dilakukan dengan skenario testing.

d. Evaluasi
Pada tahap ini dilakukan evaluasi hasil dari testing yang telah dilakukan, sejauh mana tingkat efektifitas dari teknologi keamanan yang dibangun, dan membandingkan dengan tujuan awal serta kondisi ideal yang diharapkan. Hasil dari analisa akan dijadikan sebagai masukan untuk perbaikan sistem juga sebagai saran untuk usaha perbaikan di masa yang akan datang[9].

### 3.3 Metode Pengujian Sistem

Desain Pengujian dilakukan dengan menggunakan metode eksperimen yang dimaksudkan apakah sistem Snort dapat mendeteksi serangan *Sniffing* dengan baik[10]. Pengujian dilakukan dengan menggunakan Ettercap untuk *Sniffing* yang akan dilakukan oleh komputer *Attacker* seperti terlihat pada gambar 3 dibawah ini, dan Tabel 1 menyajikan komponen pengujian sistemnya.

Gambar 3. Alur Pengujian Sistem

Tabel 1. Komponen Pengujian Sistem

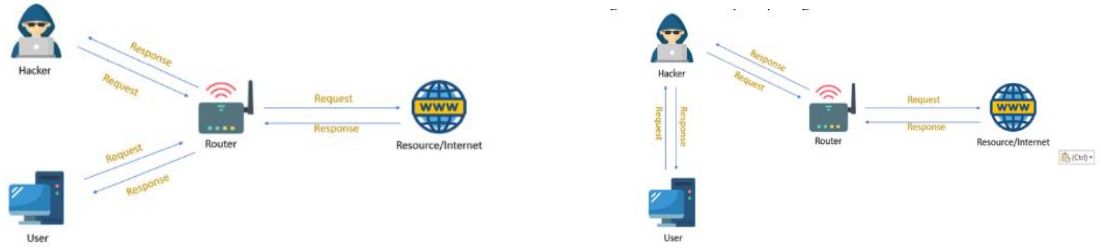
| No | Komponen Pengujian | Proses Pengujian | Hasil Pengujian |
|---|---|---|---|
| 1 | Komputer server | Kinerja *Snort* untuk deteksi *Sniffing*. | Snort dapat mendeteksi serangan yang dilakukan *client*. |
| 2 | Komputer Client | Melakukan *Sniffing* ke komputer server | Komputer client berhasil menyadap (*Sniffing*) ke komputer server |

*menggunakan Ettercap.*

## HASIL DAN PEMBAHASAN

### Desain Sistem

Pada kondisi normal, biasanya setiap user akan langsung berhubungan dengan router, akan tetapi ketika jaringan telah disadap maka topologi akan berubah. Gambar 4,a menunjukan gambaran jika kondisi jaringan dalam keadaan normal sementara gambar 4,b menunjukan kondisi jika sudah menerima serangan Sniffing.




(a) (b)

Gambar 4. (a) Kondisi Jaringan Normal, (b) Kondisi Jaringan Serangan Snifing

Konfigurasi ekperimen terhadap masing-masing komponen dapat dilihat pda tabel 2 dibawah ini :

Tabel 2. Konfigurasi Eksperimen

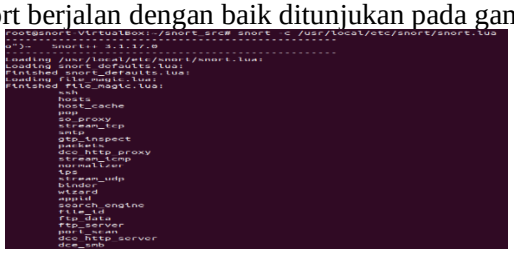
| Nama PC dan IP Address | Sistem Operasi | Tools Pendukung | Konfigurasi Aplikasi |
|---|---|---|---|
| PC1 IP:192.168.0.1 | Ubuntu versi 18.04 LTS | Snort | IDS dengan *alert* Snort *Rules* untuk deteksi *Sniffing* |
| PC2 IP:192.168.0.2 | Kali Linux | Terminal | Aplikasi Ettercap untuk menyadap (*Sniffing*) |

### Instalasi Snort

Untuk tahap pertama adalah melalukan instalasi snort 3 dan hasil instalasi tersebut ditunjukkan pada gambar 5 dibawah ini:

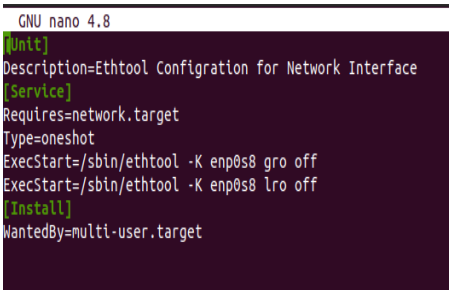

Gambar 5. Hasil Instalasi Snort

Hasil pengujian instalasi snort berjalan dengan baik ditunjukan pada gambar 6 berikut ini:

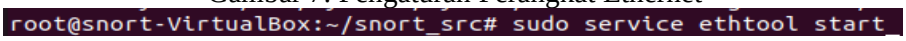


Gambar 6. Pengujian Hasil Instalasi

Gambar 7 dan gambar 8 menunjukkan konfigurasi perangkat ethernet yang akan di monitor atau diawasi oleh snort dan mengaktifkannya[11].




Gambar 7. Pengaturan Perangkat Ethernet

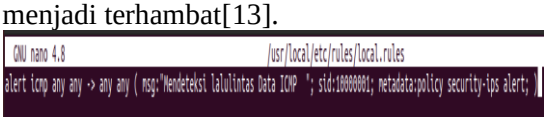



Gambar 8**.** Aktifasi Perangkat Ethernet

Gambar 9 menunjukkan direktori untuk menyimpan rule snort, rule ini digunakan untuk menyimpan perintah pada snort dalam mendeteksi serangan yang sudah didefinisikan[12].


Gambar 9. Direktori Pengaturan Snort

Gambar 10 adalah *rule* atau aturan yang penulis buat untuk mendeteksi serangan *Sniffing,* serangan *Sniffing* menggunakan paket data protokol ICMP yang dikirimkan secara *masive* sehingga server akan mengalami kelebihan paket data yang diterima sehingga menyebabkan pengguna lain yang mengakses server tersebut menjadi terhambat[13].

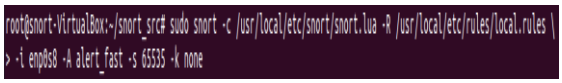



Gambar 10. Rule Snort Deteksi Sniffing

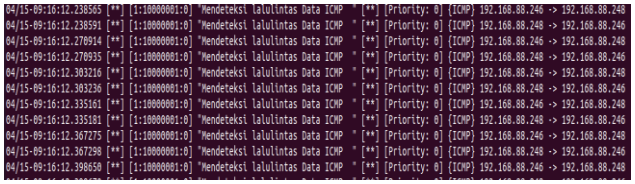
*Rule* atau aturan yang penulis buat untuk mendeteksi *ping flood* adalah dengan mendeteksi paket data ICMP yang berlebihan, dan melewati ethernet yang sudah dimasukkan dalam pengaturan snort untuk diawasi[14].

**Pengujian Sistem**

Pengujian sistem dilakukan menggunakan dua buah PC komputer, satu komputer sebagai server menggunakan sistem operasi Linux Ubuntu, dan komputer lainnya sebagai attacker menggunakan sistem operasi Kali Linux[15]. Gambar 11 dan 12 menunjukkan penggunaan *rule* untuk mendeteksi serangan *sniffing* dan hasil deteksi serangan *sniffing* pada server[16].




Gambar 11. Penerapan *rule* snort untuk mendeteksi *sniffing* secara *real time*




Gambar 12. Hasil deteksi serangan *sniffing* secara *real time*

Gambar 13 menunjukkan statistik hasil deteksi sniffing secara real time menggunakan snort. Dari gambar 13 ini dapat dilihat ip address dari computer penyerang yaitu 192.168.88.246 dengan serangan sniffing yang membanjiri lalu lintas data di protocol ICMP[17].

Gambar 13. Hasil Deteksi Serangan Sniffing

Dari pengujian yang telah dilakukan maka dapat ditarik kesimpulan sistem deteksi serangan sniffing dapat mendeteksi serangan tersebut secara real time[18].

## KESIMPULAN

Hasil dari penelitian ini berupa sistem yang dapat mendeteksi serangan packet sniffing, sehingga pihak sekolah SMPN I Muara Kelingi dapat menggambil langkah penyelamatan data dengan lebih cepat.

## UCAPAN TERIMA KASIH

Pada bagian ini bersifat optional, boleh dihilangkan oleh penulis. Ucapan terima kasih berisikan prakata apresiasi penulis kepada orang, kelompok atau instansi yang berkontribusi pada program penelitian.

## DAFTAR PUSTAKA

[1] Y. N. Kunang *et al.*, "Analysis and implementation of the Port Knocking method using Firewall-based Mikrotik RouterOS," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 8, no. 4, pp. 1907–5022, 2019.

[2] A. Umasugi, M. D. Suratin, and S. Hamza, "Analisis Keamanan Jaringan Wifi Terhadap Packet Sniffing DiKampus a Universitas Muhammadiyah Maluku Utara," *Produktif J. Ilm. Pendidik. Teknol. Inf.* , vol. 6, no. 2, pp. 597–602, 2022, [Online]. Available: https://journal.umtas.ac.id/index.php/produktif/article/view/2460

[3] C. A. Putra, M. S. Munir, Y. V. Via, and R. Achmadipoetro, "Deteksi Serangan Trojan Horse Dengan Memanfaatkan Ids Snort," *Semin. Santika*, no. September, pp. 203–206, 2019, [Online]. Available: http://santika.ijconsist.org/index.php/SANTIKA/article/view/31

[4] M. A. S. Arifin, "Rancang Bangun Prototype Robot Lengan Menggunakan Flex Sensor Dan Accelerometer Sensor Pada Lab Mikrokontroler Stmik Musirawas," *Ilk. J. Ilm.*, vol. 9, no. 3, pp. 255–261, 2017, doi: 10.33096/ilkom.v9i3.152.255-261.

[5] R. Sahara, S. Abdullah, and R. Saputra, "Analisis Ancaman Sniffing pada Jaringan WiFi di PT. Stepa Wirausaha Adiguna," *Pros. Semin. Nas. Ris. Dan Inf. Sci.*, vol. 4, pp. 224–230, 2022.

[6] R. Kurniawan and A. Zulius, "Sistem Smart Parking Menggunakan Ultrasonik Sensor," *J. Sist. Komput. Musirawas*, vol. 3, no. 1, p. 22, 2018, doi: 10.32767/jusikom.v3i1.309.

[7] B. Wijaya and A. Pratama, "Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (Ids) Berbasis Snort," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 1, pp. 97–101, 2020, doi: 10.32736/sisfokom.v9i1.770.

[8] Ilham Firdaus, Januar Al Amien, and S. Soni, "String Matching untuk Mendeteksi Serangan Sniffing (ARP Spoofing) pada IDS Snort," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 1, no. 2, pp. 44–49, 2020, doi: 10.37859/coscitech.v1i2.2180.

[9] W. Fathoni, Fitriyani, and G. N. Nurkahfi, "Deteksi Penyusupan Pada Jaringan Komputer Menggunakan Ids Snort," *e-Proceeding Eng.*, vol. 3, no. 1, pp. 1169–1172, 2016, [Online]. Available: https://openlibrary.telkomuniversity.ac.id/pustaka/files/114823/persembahan/deteksi-penyusupan-pada-jaringan-komputer-menggunana-ids-snort.pdf

[10] A. Rizal Fauzi and I. Made Suartana, "Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids," *J. Manaj. Inform.*, vol. 8, no. 2, p. 7, 2018.

[11] A. Akhriana and A. Irmayana, "Web App Pendeteksi Jenis Serangan Jaringan Komputer Dengan Memanfaatkan Snort Dan Log Honeypot," *CCIT J.*, vol. 12, no. 1, pp. 85–96, 2019, doi: 10.33050/ccit.v12i1.604.

[12] T. Widodo and A. S. Aji, "Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS)," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 1, pp. 46–55, 2022, doi: 10.14421/jiska.2022.7.1.46-55.

[13] A. Prasetyo, L. Affandi, and D. Arpandi, "Implementasi Metode Naive Bayes Untuk Intrusion Detection System (Ids)," *J. Inform. Polinema*, vol. 4, no. 4, p. 280, 2018, doi: 10.33795/jip.v4i4.220.

[14] Sutarti, A. P. Pancaro, and F. I. Saputra, "Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal," *J. PROSISKO*, vol. 5, no. 1, pp. 1–8, 2018.

[15] R. Suwanto, I. Ruslianto, and M. Diponegoro, "Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IPTable Pada Monitoring Jaringan Lokal Berbasis Website," *J. Komput. dan Apl.*, vol. 07, no. 1, pp. 97–107, 2019.

[16] J. Fahana, R. Umar, and F. Ridho, "Pemanfaatan Telegram Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan," *J. Sist. Inf.*, vol. 5341, no. 6, p. 2, 2017.

[17] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 413, 2020, doi: 10.30865/mib.v4i2.2037.

[18] S. Alviana and I. D. Sumitra, "Analisis Pengukuran Penggunaan Sumber Daya Komputer Pada Intrusion Detection System Dalam Meminimalkan Serangan Jaringan," *Komputa J. Ilm. Komput. dan Inform.*, vol. 7, no. 1, pp. 27–34, 2018, doi: 10.34010/komputa.v7i1.2533.