

Perancangan *Prototype* Sistem Pendeteksi Penyusup Perimeter Bandar Udara dengan Metode *Fuzzy Logic* Berbasis *Internet of Things*

I Made Yogaswara Dipta¹, Ni Made Ary Esta Dewi Wirastuti², Ngurah Indra ER³

[Submission: 19-12-2023, Accepted: 19-03-2024]

Abstract— Aviation Security is a condition that provides protection to aviation from Unlawful Act of Interference through a combination of human resources, procedures, facilities. There are various types of unlawful acts in the aviation, one of them is entering the Restricted Security Area, or the aeronautical facility area illegally, such as the case of "Mario" who intruding the airport perimeter so that he could enter the wheels of Garuda Indonesia's aircraft in 2015. To prevent similar incidents, it is necessary to implement aviation security facilities with the latest technology to anticipate intruders entering the Restricted Security Area. One of them is the perimeter intruder detection system (PIDS). In this research, an IOT-based PIDS was designed using fuzzy logic method. Based on testing, the performance of the Perimeter Intruder Detection System (PIDS) was analyzed using the confusion matrix method and it can be stated that the designed prototype of the perimeter intruder detection system has good accuracy/good classification (83.33%).

Intisari— Keamanan Penerbangan merupakan suatu kondisi untuk melindungi penerbangan dari Tindakan Melawan Hukum melalui perpaduan antara pemanfaatan sumber daya manusia, prosedur dan fasilitas. Terdapat berbagai jenis tindakan melawan hukum dalam dunia penerbangan salah satunya adalah memasuki Daerah Keamanan Terbatas, atau area aeronautika secara tidak sah seperti kasus "Mario" yang melakukan penyusupan perimeter bandar udara sehingga masuk ke roda pesawat Garuda Indonesia pada tahun 2015. Untuk mencegah terjadinya kejadian serupa, maka perlu diterapkan fasilitas keamanan penerbangan dengan teknologi terkini untuk mengantisipasi adanya penyusup yang memasuki Daerah Keamanan Terbatas. salah satunya adalah sistem deteksi penyusup perimeter (PIDS). Dalam penelitian ini, dilakukan perancangan PIDS berbasis IoT dengan menggunakan metode *fuzzy logic*. PIDS yang dirancang menggunakan mikrokontroler Node MCU ESP8266 dan dilengkapi sensor PIR untuk mendeteksi pergerakan manusia, sensor ultrasonik untuk mengukur jarak, kamera ESP-32, relay, indikator *buzzer*. Berdasarkan pengujian skenario, kinerja dari dianalisis menggunakan metode *confusion matrix* dan dapat dinyatakan bahwa *prototype* sistem pendeteksi penyusup perimeter yang dirancang memiliki akurasi yang baik/good classification (83.33%).

Kata Kunci— Keamanan Penerbangan, Perimeter Intruder Detection System (PIDS), Logika Fuzzy, *Internet of Things*

I. PENDAHULUAN

Keamanan Penerbangan adalah suatu kondisi untuk melindungi penerbangan dari tindakan yang melanggar hukum melalui perpaduan penggunaan sumber daya manusia, prosedur, dan fasilitas. Tindakan melanggar hukum yang dimaksud salah satunya yakni memasuki pesawat udara, dan daerah keamanan terbatas bandara secara tidak sah [1], seperti kasus "Mario" yang berhasil menerobos perimeter bandara sehingga dapat masuk ke dalam roda pesawat Garuda Indonesia pada tahun 2015. Dalam Annex 14 tentang *Aerodromes*, Organisasi Penerbangan Sipil Internasional (ICAO) merekomendasikan perlunya pemagaran di daerah keamanan terbatas. Setiap bandara harus dibangun perimeter yang merupakan pagar atau pembatas sebagai upaya preventif terhadap masuknya hewan besar dan orang yang tidak berkepentingan ke dalam daerah keamanan terbatas karena dapat membahayakan keamanan penerbangan di bandara tersebut [2]. Gambar 1 menunjukkan contoh pagar perimeter sebagai perlindungan fisik daerah keamanan terbatas di bandara.



Gambar 1: Perimeter bandar udara

Menurut Keputusan Direktur Jenderal Perhubungan Udara – Kementerian Perhubungan RI No: KP 138 Tahun

¹ Mahasiswa, Program Studi Magister Teknik Elektro Fakultas Teknik Universitas Udayana, Jln. Kampus Bukit Jimbaran 80361 INDONESIA (telp: 0361-703315; fax: 0361-4321; e-mail: diptyogaswara@gmail.com)

^{2, 3} Dosen, Program Studi Magister Teknik Elektro Fakultas Teknik Universitas Udayana, Jln. Kampus Bukit Jimbaran 80361 INDONESIA (telp: 0361-703315; fax: 0361-4321; e-mail: dewi.wirastuti@unud.ac.id, indra@unud.ac.id)



2018 tentang Sertifikasi Peralatan Keamanan, operator bandara wajib menyediakan pos pemeriksaan keamanan untuk akses ke sisi udara dan memiliki fasilitas keamanan penerbangan, salah satunya adalah sistem pendeteksi penyusup perimeter (*perimeter intruder detection system/PIDS*) [3]. PIDS adalah sebuah alat untuk mendeteksi keberadaan penyusup yang mencoba menerobos perimeter fisik dari sebuah properti, bangunan, atau area aman lainnya. PIDS biasanya digunakan sebagai bagian dari sistem keamanan secara keseluruhan dan ditemukan di lingkungan dengan keamanan tinggi seperti lembaga masyarakat, bandara, pangkalan militer, dan pembangkit listrik tenaga nuklir [4]. Pengadaan fasilitas PIDS pada bandara di Indonesia secara umum belum diimplementasikan dengan masif karena membutuhkan biaya investasi peralatan yang tinggi. Produk PIDS yang beredar di pasar internasional saat ini dijual dengan kisaran harga sekitar USD 125 per unit dengan fitur pengiriman notifikasi melalui SMS [21].

Beberapa tinjauan terbaru telah dilakukan terkait dengan penerapan konsep *internet of things (IoT)* terhadap sistem pendeteksi penyusup manusia [5]-[7],[20],[23]. Xie Z, dkk [5] mengusulkan *framework* pendeteksi penyusup perimeter lintasan kereta cepat berbasis IoT, penelitian ini dirancang untuk mengintegrasikan hasil pembacaan sensor yang terpasang di beberapa titik. Algoritma *data fusion* digunakan untuk menggabungkan data multisensor guna meningkatkan keakuratan pendeteksian. Hoang ML [6] mengusulkan metodologi baru untuk menggabungkan pembacaan sensor berdasarkan aturan HMM (model *hidden markov*). Rambabu, Kalathiripi [7] membangun suatu sistem dengan prinsip kerja apabila terdapat penyusup maka sistem akan membandingkan data penyusup tersebut dengan *database* yang tersedia pada sistem. Jika teridentifikasi adanya penyusup maka sistem akan memberikan notifikasi kepada pengguna melalui SMS atau email. Penerapan IoT lainnya dilakukan oleh Abdullah, dkk [20] menggunakan kombinasi sensor inframerah untuk mendeteksi manusia dan mengirimkan pemberitahuan ke antarmuka pengguna berbasis IoT. Selain itu, Sutikno, dkk [23] merancang *prototype* sistem pemantauan debit air dengan nilai akurasi yang relatif baik dan penggunaan energi listrik yang efisien.

Metode pengambilan keputusan yang umum digunakan dalam sebagai solusi dalam topik ini salah satunya adalah metode *neural network* [8][9]. S. Yasukawa dan M. Kim [8] merancang sistem deteksi penyusup yang menggunakan karakteristik *spatiotemporal* dari *microwave multipath propagation*. P Shirin Saleem dkk [9] mengimplementasikan algoritma *machine learning* dengan masukan berupa video *real-time* dan mendeteksi keberadaan penyusup di lokasi untuk selanjutnya dikirimkan kepada pengguna. Model ini menggunakan *Convolutional Neural Networks* dan dilatih menggunakan *dataset* rekaman CCTV sebagai masukan. Beberapa peneliti juga menggunakan metode berbasis *image processing* [7],[10],[11],[16]. Rambabu, Kalathiripi [7] membangun sebuah sistem dimana citra diperoleh dan dianalisis melalui perbandingan *frame* yang diubah menjadi citra *grayscale*, kemudian difilter melalui serangkaian penyempurnaan citra VI. N. Chandra dan SP Panda [10] menggunakan model YOLO untuk mendeteksi objek manusia dalam video yang diambil oleh

kamera dengan resolusi standar. Sejumlah eksperimen dilakukan untuk mengevaluasi kinerja model. Prabu dan P. Susakar [11] melakukan penelitian untuk mendeteksi dan mengklasifikasikan objek dengan algoritma *deep learning* khususnya dengan *Content-Based Image Retrieval (CBIR)*, gambar yang diambil diklasifikasikan berdasarkan fitur yang diekstraksi. Almonfrey D, dkk [16] melakukan penelitian yang memanfaatkan sistem multi-kamera. Untuk memvalidasi pendekatan ini, peneliti menerapkan tiga skenario berbeda sebagai pembuktian terhadap konsep yang diajukan.

Disamping menggunakan kamera untuk memperoleh data, beberapa peneliti juga menggunakan sensor *infrared* untuk mendeteksi pergerakan manusia [12]-[13]. D. Arjun, dkk [12] mengusulkan sistem *multi-sensing* yang terdiri dari sensor inframerah untuk mendeteksi pergerakan penyusup yang melintasi suatu pembatas. Pada pengembangannya, D. Arjun, dkk [13] meningkatkan akurasi sistem pada daerah perbatasan yang datar, daerah perbatasan dengan penyeberangan sungai atau kolam, daerah perbatasan yang ditutupi oleh dedaunan dan daerah perbatasan yang ditutupi oleh dedaunan kering. Beberapa penelitian lain menggunakan *wave signals* untuk mendeteksi adanya penyusup [14], [15]. Peijun Zhao, dkk [14] mengusulkan sistem pelacakan dan identifikasi manusia berdasarkan radar *millimeter-wave* untuk membentuk lintasan yang berhubungan secara temporal. S. Yasukawa dan M. Kim [15] menyajikan hasil evaluasi kinerja sistem pendeteksi manusia dengan berbagai parameter pengukuran seperti bentuk susunan antena dan *bandwidth* sinyal di lokasi jalur propagasi yang digunakan.

Metode pengambilan keputusan yang populer digunakan oleh para peneliti yakni logika *fuzzy* seperti Siti Dewi Dayanti Harahap [18] yang dalam penelitiannya, logika *fuzzy* dapat membantu mendefinisikan karakteristik operasional suatu sistem dan juga untuk pengambilan keputusan dalam penyelesaian masalah. Putra, dkk [22] merancang sistem pengambilan keputusan berbasis Fuzzy Tsukamoto karena metode ini memiliki efisiensi pada penentuan aturan dan pemrosesan data yang memiliki *taboo range* dan menghasilkan *output craps*. Penelitian dengan topik pendeteksian manusia dengan Node MCU dan logika *fuzzy* pernah dilaksanakan oleh Aldisa dan Alfarisi [24], yang membangun sebuah alat pendeteksi keamanan ruangan menggunakan sensor PIR. Dalam penelitian ini, peneliti berhasil menunjukkan bahwa alat mampu melakukan pendeteksian penyusup.

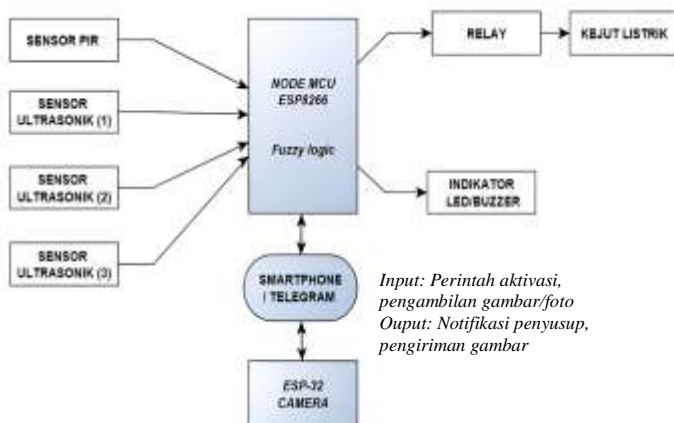
Berdasarkan penelitian-penelitian yang telah dilaksanakan sebelumnya, dapat diketahui bahwa penelitian terdahulu [24] hanya mampu melakukan pendeteksian penyusup ke suatu ruangan tanpa disertai fitur keamanan tambahan dan tidak dilakukan pengujian skenario beserta analisis kinerja dari alat yang dibuat. Disamping itu, PIDS yang dijual di pasaran saat ini relatif mahal [21] dengan minim fitur keamanan. Oleh karena itu, pada penelitian ini penulis merancang suatu sistem pendeteksi penyusup perimeter (*pids*) dengan biaya yang rendah disertai penambahan fitur-fitur keamanan berupa kejut listrik (*electric shocks*) dan pengambilan gambar obyek deteksi dari jarak jauh dengan *smartphone* sebagai upaya pencegahan

terjadinya penyusupan ke daerah keamanan terbatas bandar udara. *Prototype* PIDS yang dirancang menggunakan logika *fuzzy* untuk menentukan variabel *input* sehingga dapat ditentukan apakah obyek yang dideteksi oleh sensor PIR dan beberapa sensor ultrasonik dikategorikan sebagai penyusup. Kinerja dari perangkat ini dianalisis berdasarkan data yang diperoleh dari pengujian skenario dengan menggunakan metode *confusion matrix*.

II. METODE PENELITIAN

A. Perancangan sistem hardware

Alat yang dirancang merupakan sebuah perangkat yang memiliki fungsi utama untuk melakukan pendeteksian terhadap penyusup (manusia) ke daerah keamanan terbatas di bandar udara berbasis *Internet of Things (IoT)*. *Software* yang digunakan dalam pemrograman mikrokontroler Node MCU dan ESP-32 *camera* adalah Arduino IDE, sementara itu untuk antarmuka komunikasi pengguna dan perangkat, penulis menggunakan aplikasi Telegram. Berdasarkan pendeteksian yang dilakukan oleh sensor, dan selanjutnya diproses oleh mikrokontroler, perangkat dapat menentukan adanya penyusup ke suatu area dan memberikan pemberitahuan ke *smartphone* melalui aplikasi telegram serta dapat disertai gambar/foto di area sekitar perangkat terpasang. Adapun *input* dari perangkat ini meliputi 1 (satu) buah sensor PIR (*motion sensor*), 3 (tiga) buah sensor ultrasonik HC-SR04, kamera, dan perintah dari aplikasi telegram. *Input* tersebut akan diolah oleh unit kendali sesuai dengan program yang ditanamkan pada mikrokontroler sehingga menghasilkan *output* berupa tindakan/respon dimana apabila obyek yang terdeteksi dinyatakan sebagai penyusup, maka perangkat akan mengirimkan notifikasi serta gambar/foto area sekitar perangkat ke aplikasi telegram. Disamping itu, perangkat akan mengaktifkan relay sehingga mengalirkan arus listrik ke pagar perimeter sebagai efek kejut untuk menunda upaya penyusupan. Dalam hal ini, perangkat juga akan mengaktifkan indikator *buzzer* sebagai peringatan langsung. Diagram blok dari sistem alat ini secara umum ditunjukkan pada Gambar 2.



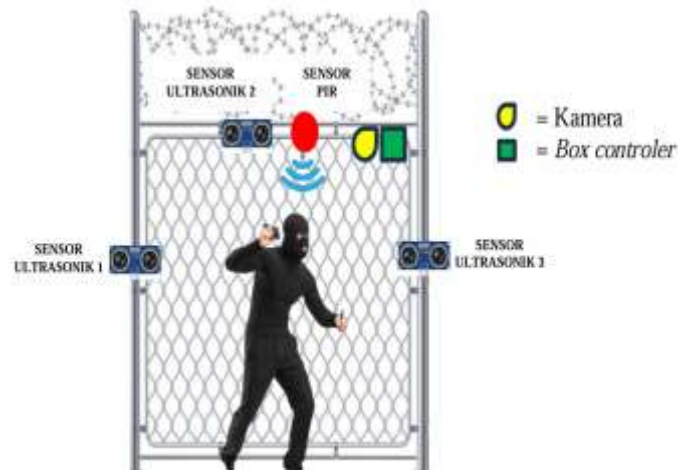
Gambar 2: Diagram blok sistem alat

Perancangan sistem *hardware* pada alat ini membutuhkan berbagai komponen elektronika. Modul Node MCU digunakan sebagai unit kendali karena bersifat *open source* dengan harga

yang relatif lebih murah dibandingkan unit kendali lain, sehingga *output* alat yang dihasilkan memiliki harga yang lebih terjangkau ketika dipasarkan. Selain itu, Node MCU memiliki banyak perangkat pendukung yang *compatible* sehingga pengguna dapat merancang alat yang lebih kreatif.

Dalam perancangan ini, digunakan sensor *Passive Infrared (PIR)* karena sensor ini secara spesifik hanya merespon apabila mendeteksi energi panas inframerah yang terpancar dari tubuh manusia/hewan sehingga dapat memperkecil peluang kesalahan pendeteksian obyek selain manusia/hewan. Dalam hal ini, digunakan sensor PIR sebanyak 1 (satu) buah yang ditempatkan di bagian atas pagar perimeter. Berdasarkan eksperimen sensor pergerakan (PIR), bisa diketahui bahwa sensor PIR mampu mendeteksi pergerakan seseorang dengan rentang jarak sejauh 4,5 meter dan jangkauan posisi obyek sebesar 45° hingga 315° dari bagian depan sensor. Sehingga hanya dengan pemasangan 1 (satu) buah sensor PIR, dapat menjangkau area pagar perimeter. Untuk mengukur jarak antara pagar perimeter dengan manusia, digunakan sensor ultrasonik HC-SR04. Pemasangan sensor ultrasonik ini diposisikan di bagian kanan, kiri, serta tengah untuk mengidentifikasi jarak manusia saat berupaya menyusup di pagar perimeter.

Perangkat ini dilengkapi dengan kamera yang dapat mengambil gambar untuk dikirimkan ke aplikasi telegram pada *smartphone* via jaringan wi-fi. Untuk menjalankan fungsi kejut listrik, maka perangkat akan mengaktifkan *relay* sehingga arus listrik akan mengalir pada pagar perimeter yang bersifat konduktor listrik. Adapun gambaran penempatan alat pada pagar perimeter seperti yang ditunjukkan pada Gambar 3.

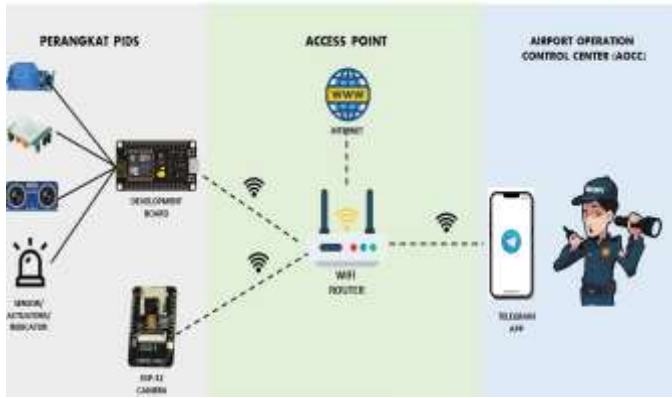


Gambar 3: Titik pemasangan perangkat

Perangkat ini dilengkapi dengan kamera yang dapat *capture* gambar untuk dikirimkan ke aplikasi telegram pada *smartphone* via jaringan wi-fi. Untuk menjalankan fungsi kejut listrik, maka perangkat akan mengaktifkan relay sehingga arus listrik akan mengalir pada pagar perimeter yang bersifat konduktor listrik.

Adapun alur komunikasi *internet of things* terdiri atas tiga *locus* penting yakni perangkat PIDS, *access point*, serta *airport security control room* seperti yang ditampilkan pada Gambar 4.





Gambar 4: Alur komunikasi internet of things

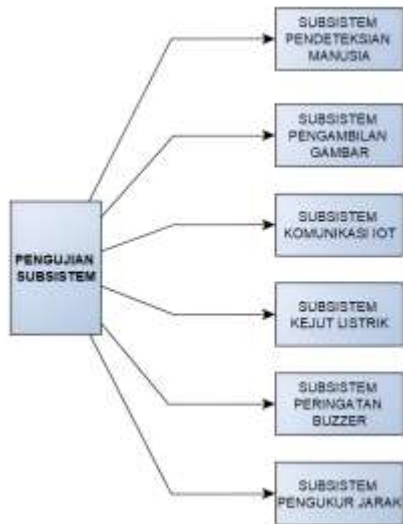
Perangkat PIDS yang terdiri atas sensor-sensor melakukan fungsi pendeteksian penyusup, kemudian *access point* sebagai titik akses untuk perangkat akan menyediakan jaringan internet sehingga data berupa respon sensor dari perangkat PIDS dapat disampaikan kepada petugas *aviation security* yang berada di *airport operation control center* (AOCC) melalui aplikasi telegram pada *smartphone*.

B. Perancangan sistem software

Tahapan ini bertujuan untuk merancang pemrograman mikrokontroler Node MCU pada *environment* yang telah tersedia serta *platform IoT* yang digunakan. Dalam tahap ini, akan dilakukan pemrograman untuk pengujian subsistem sebelum diimplementasikan dalam satu sistem yang terintegrasi.

1. Pengujian subsistem

Pengujian subsistem dilakukan untuk mengetahui kinerja dari subsistem yang dibagi menjadi beberapa blok pengujian seperti yang ditunjukkan pada Gambar 5.

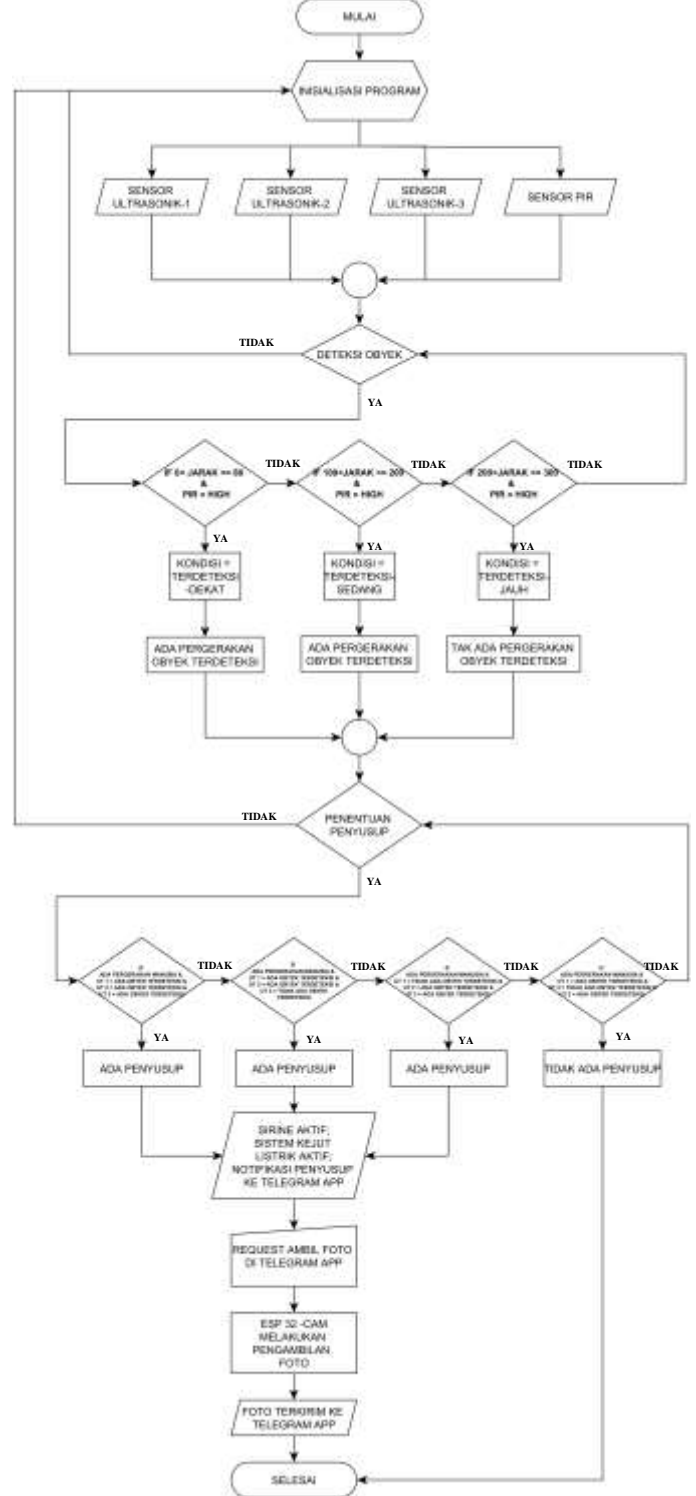


Gambar 5: Blok diagram pengujian subsistem

C. Pembuatan alat dan implementasi software ke hardware

Implementasi *software* ke *hardware* pada perangkat dilakukan setelah *software* dan *hardware* telah dinyatakan berfungsi dengan baik melalui pengujian-pengujian yang dilakukan pada penelitian ini, sehingga perangkat yang akan dibangun diharapkan memiliki performa yang baik dan berfungsi sesuai dengan perencanaan.

Adapun alur kerja dari sistem yang dirancang yakni seperti ditunjukkan pada Gambar 6.



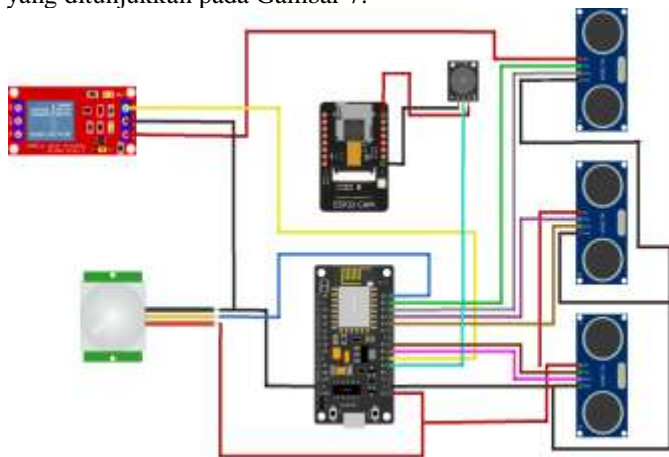
Gambar 6: Alur kerja sistem

Adapun *flowchart* dari PIDS dapat dijabarkan sebagai berikut:

- 1) Fungsi pendeteksian obyek bekerja untuk mengidentifikasi adanya penyusup melalui 1 (satu) buah sensor pergerakan (sensor PIR) dan 3 (tiga) buah sensor ultrasonik. Berdasarkan hasil pembacaan sensor-sensor yang terpasang pada perangkat, maka hasil pembacaan sensor didasarkan pada Tabel 1.

- 2) Fungsi penentuan penyusup
Berdasarkan hasil pendeteksian obyek, maka dapat ditentukan obyek yang terdeteksi dikategorikan penyusup sesuai dengan aturan yang disajikan pada Tabel 3.
- 3) Apabila sistem mendeteksi adanya penyusup sesuai ketentuan pada Tabel 3 maka sistem kejut listrik akan bekerja dengan mengaktifkan relay dari *normally open* (NO) menjadi *close circuit* sehingga arus listrik dapat dialirkan pada pagar perimeter sebagai upaya menunda aksi penyusupan
- 4) Selanjutnya indikator *buzzer* dengan bunyi sirine akan aktif agar orang-orang yang berada disekitar perimeter dapat memberikan perhatian lebih pada sumber suara.
- 5) Sistem akan mengirimkan pemberitahuan berupa notifikasi adanya penyusup ke aplikasi telegram yang dapat dipantau petugas keamanan
- 6) Dalam hal memastikan keadaan sebenarnya di titik pemasangan PIDS, petugas keamanan dapat melakukan request untuk pengambilan gambar melalui aplikasi Telegram.
- 7) Kamera ESP-32 melakukan pengambilan gambar selanjutnya dikirimkan ke aplikasi telegram.

Berdasarkan daftar pin *input* dan *output* yang telah ditentukan, maka dapat digambarkan diagram skematik seperti yang ditunjukkan pada Gambar 7.



Gambar 7: Diagram skematik alat

D. Pengujian skenario

Uji skenario dilaksanakan dengan maksud untuk mengetahui beberapa kemungkinan yang dapat terjadi ketika alat melakukan pendeteksian penyusup. Adapun beberapa pengujian skenario antara lain:

1. Skenario I

Pada skenario ini, seseorang memanjat dari sisi kanan pagar perimeter, dengan posisi berdekatan dengan sensor ultrasonik-3 (bagian kanan) namun jauh dari sensor ultrasonik-1 (bagian kiri).

2. Skenario II

Pada skenario ini, seseorang memanjat dari sisi kanan pagar perimeter, dengan posisi berdekatan dengan sensor ultrasonik-3 (bagian kanan) namun jauh dari sensor ultrasonik-1 (bagian kiri)

3. Skenario III

Pada skenario ini, seseorang memanjat dari bagian tengah pagar perimeter, dengan jarak orang ke sensor ultrasonik pada sisi kanan dan sisi kiri adalah sama.

E. Penerapan logika fuzzy

Algoritma *fuzzy* diterapkan untuk memetakan ruang *input* ke dalam ruang *output*.

1. Masukan *crisp*

Nilai masukan berupa jarak yang diukur oleh sensor ultrasonik, terdiri atas jarak dekat, sedang, dan jauh seperti yang disajikan pada Tabel 1.

TABEL 1
INPUT CRISP SENSOR

JARAK	INPUT SENSOR		KETERANGAN
	PIR	ULTRASONIK	
Dekat	High	$0 < \text{jarak objek} \leq 100$ cm	Ada pergerakan obyek terdeteksi
Sedang	High	$100 < \text{jarak objek} \leq 200$ cm	Ada pergerakan obyek terdeteksi
Jauh	High	$200 < \text{jarak objek} \leq 300$ cm	Tidak Ada pergerakan obyek terdeteksi

2. Fuzzyfikasi

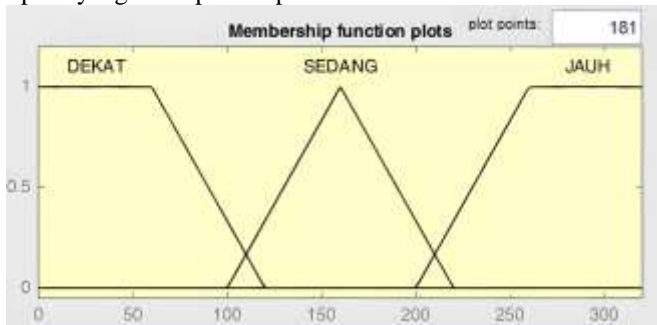
Berdasarkan nilai *input* yang diperoleh dari pembacaan sensor, maka dilakukan proses *fuzzification* dengan tujuan memperoleh nilai derajat keanggotaan. Dalam penelitian ini, terdapat dua fungsi keanggotaan (*membership function*) yaitu fungsi keanggotaan *input* sensor, dan fungsi keanggotaan *output* status penyusup. Fungsi keanggotaan *input* sensor ultrasonik 1,2, dan 3 mempunyai jenis masukan yang sama yaitu jarak objek pada sensor. Jarak ini terdiri atas 3 (tiga) himpunan *fuzzy* yakni dekat, sedang, dan jauh. Adapun fungsi keanggotaan *output* status penyusup mempunyai 2 (dua) himpunan *fuzzy* yakni ada penyusup dan tidak ada penyusup. Himpunan *fuzzy* dari setiap variabel dapat disajikan pada Tabel 2.

TABEL 2I
HIMPUNAN FUZZY

Jenis	Variabel penelitian	Himpunan fuzzy	Nilai	Params M.F	Tipe M.F
Input	Jarak	a. Dekat	[0-120]	[0 0 60 120]	Trapmf
		b. Sedang	[100-220]	[100 160 220]	Trimf
		c. Jauh	[200-320]	[200 260 320 320]	Trapf
Output	Status	a. Ada penyusup	[0-220]	[0 0 110 220]	Trapmf
		b. Tidak ada penyusup	[200-320]	[200 260 320 320]	Trapmf



Fungsi keanggotaan dari *input* sensor ultrasonik menerapkan jenis kurva segitiga (*trimf*) dan trapesium (*trapmf*) seperti yang ditampilkan pada Gambar 8.



Gambar 8: Fungsi Keanggotaan Masukan dari Sensor Ultrasonik

Adapun penjabaran dari fungsi keanggotaan *input* sensor ultrasonik yakni sebagai berikut:

$$\mu_{dekat} = \begin{cases} 1 & ; x \leq 60 \\ \frac{(120-x)}{(120-60)} & ; 60 \leq x \leq 120 \\ 0 & ; x \geq 120 \end{cases}$$

$$\mu_{sedang} = \begin{cases} 0 & ; x \leq 100 \text{ atau } x \geq 220 \\ \frac{(x-100)}{(160-100)} & ; 100 \leq x \leq 160 \\ \frac{(160-x)}{(220-160)} & ; 160 \leq x \leq 220 \end{cases}$$

$$\mu_{banyak} = \begin{cases} 0 & ; x \leq 220 \\ \frac{(x-200)}{(260-220)} & ; 200 \leq x \leq 260 \\ 1 & ; 160 \leq x \leq 260 \end{cases}$$

3. Evaluasi Aturan (*Rule Evaluation*)

Adapun logika yang digunakan untuk penentuan adanya penyusup pada *prototype* PIDS yang dirancang disajikan pada Tabel 3.

TABEL 3
LOGIKA PENENTUAN PENYUSUP

Nama sensor	STATUS INPUT			
	Kondisi I	Kondisi II	Kondisi III	Kondisi IV
PIR	Ada pergerakan manusia	Ada pergerakan manusia	Ada pergerakan manusia	Ada pergerakan manusia
Ultrasonik 1	Ada obyek terdeteksi	Ada obyek terdeteksi	Tidak ada obyek terdeteksi	Ada obyek terdeteksi
Ultrasonik 2	Ada obyek terdeteksi	Ada obyek terdeteksi	Ada obyek terdeteksi	Tidak ada obyek terdeteksi
Ultrasonik 3	Ada obyek terdeteksi	Tidak ada obyek terdeteksi	Ada obyek terdeteksi	Ada obyek terdeteksi
Kesimpulan	Penyusup	Penyusup	Penyusup	Penyusup

III. HASIL DAN PEMBAHASAN

A. Hasil pengujian subsistem

1. Pengujian subsistem pendeteksi manusia

Pengujian subsistem pendeteksi manusia berfokus pada pengujian sensor PIR untuk mengetahui kinerja dan jarak maksimal obyek yang dapat dideteksi oleh sensor. Pada skenario pengujian pertama, dilakukan variasi terhadap jarak antara sensor PIR dan obyek deteksi dengan sudut konstan 0 derajat. Berdasarkan pengujian subsistem pendeteksi manusia

yang dilakukan, diperoleh hasil sesuai yang ditampilkan pada Tabel 4.

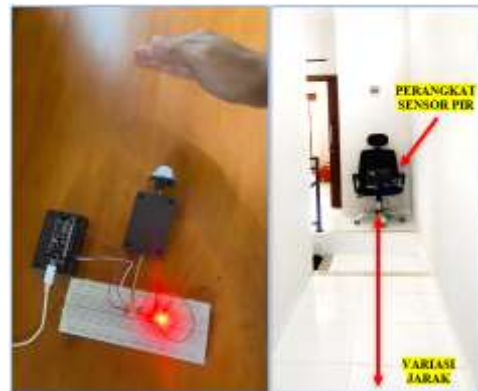
TABEL 4
HASIL PENGUJIAN SUBSISTEM PENDETEKSI MANUSIA (SKENARIO I)

Jarak (cm)	Percobaan-1	Percobaan-2	Percobaan-3
50	Terdeteksi	Terdeteksi	Terdeteksi
100	Terdeteksi	Terdeteksi	Terdeteksi
150	Terdeteksi	Terdeteksi	Terdeteksi
200	Terdeteksi	Terdeteksi	Terdeteksi
250	Terdeteksi	Terdeteksi	Terdeteksi
300	Terdeteksi	Terdeteksi	Terdeteksi
350	Terdeteksi	Terdeteksi	Terdeteksi
400	Terdeteksi	Terdeteksi	Terdeteksi
450	Terdeteksi	Terdeteksi	Terdeteksi
500	Tidak terdeteksi	Tidak terdeteksi	Tidak terdeteksi

Pada skenario pengujian kedua, dilakukan variasi terhadap posisi sudut obyek dengan jarak konstan. Berdasarkan pengujian skenario kedua, didapatkan hasil uji sesuai dengan yang ditampilkan pada Tabel 5.

TABEL 5
HASIL PENGUJIAN SUBSISTEM PENDETEKSI MANUSIA

Posisi	Percobaan-1	Percobaan-2	Percobaan-3
90°	Tidak terdeteksi	Tidak terdeteksi	Tidak terdeteksi
45°	Terdeteksi	Terdeteksi	Terdeteksi
0°	Terdeteksi	Terdeteksi	Terdeteksi
315°	Terdeteksi	Terdeteksi	Terdeteksi
270°	Tidak terdeteksi	Tidak terdeteksi	Tidak terdeteksi



Gambar 9: Pelaksanaan pengujian subsistem pergerakan manusia

Pada sensor PIR yang digunakan dalam perancangan ini, terdapat potensiometer untuk mengatur tingkat sensitivitas pendeteksian sensor. Dalam hal ini, sensor PIR digunakan dalam tingkat sensitivitas yang maksimal. Setelah dilakukan pengujian maka dapat diketahui hasil pengamatan yang ditampilkan pada Tabel 4 dan Tabel 5. Berdasarkan data pengujian tersebut, maka dapat disimpulkan bahwa sensor yang digunakan memiliki jarak deteksi maksimal sejauh 4,5 m dengan jangkauan posisi obyek pada 90° hingga 315° dari bagian depan sensor.

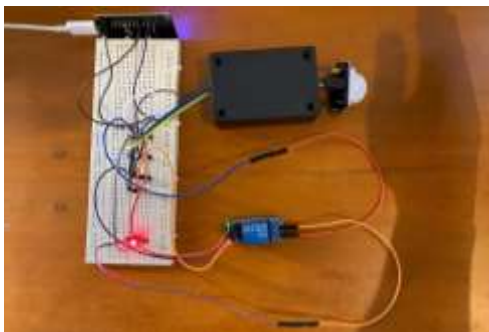
2. Pengujian subsistem kejut listrik

Pengujian subsistem kejut listrik berfokus pada pengujian terhadap respon relay. Pada skenario pengujian, dilakukan variasi terhadap jarak antara sensor PIR dan obyek deteksi dengan sudut konstan 0 derajat selanjutnya diamati respon relay

terhadap hasil pembacaan sensor PIR. Berdasarkan pengujian terhadap subsistem kejut listrik, diperoleh data sebagaimana yang ditampilkan pada Tabel 6.

TABEL 6
HASIL PENGUJIAN SUBSISTEM KEJUT LISTRIK

Jarak (cm)	Respon sensor PIR	Respon relay
50	Terdeteksi	High
100	Terdeteksi	High
150	Terdeteksi	High
200	Terdeteksi	High
250	Terdeteksi	High
300	Terdeteksi	High
350	Terdeteksi	High
400	Terdeteksi	High
450	Terdeteksi	High
500	Tidak terdeteksi	Low



Gambar 10: Pelaksanaan pengujian subsistem kejut listrik

Hasil pengamatan terhadap pengujian subsistem kejut listrik disajikan pada Tabel 6. Berdasarkan data pengujian subsistem, maka dapat diperoleh kesimpulan bahwa relay yang diuji dapat berfungsi sesuai dengan program berdasarkan *input* dari hasil pembacaan sensor PIR.

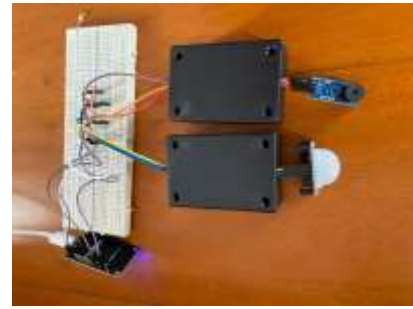
3. Pengujian subsistem peringatan buzzer

Pengujian subsistem peringatan *buzzer* berfokus pada pengujian terhadap respon *buzzer*. Pada skenario pengujian, dilakukan percobaan dengan menempatkan obyek di depan sensor PIR dengan jarak yang konstan hingga sensor PIR mendeteksi adanya pergerakan. Percobaan ini dilakukan sebanyak 10 (sepuluh) kali percobaan, selanjutnya diamati respon *buzzer* terhadap hasil pembacaan sensor PIR. Berdasarkan pengujian subsistem peringatan *buzzer*, didapatkan data sebagaimana yang ditampilkan pada Tabel 7.

TABEL 7
HASIL PENGUJIAN SUBSISTEM PERINGATAN BUZZER

Percobaan-	Respon sensor PIR	Respon buzzer
1	Terdeteksi	Berbunyi
2	Terdeteksi	Berbunyi
3	Terdeteksi	Berbunyi
4	Terdeteksi	Berbunyi
5	Terdeteksi	Berbunyi
6	Terdeteksi	Berbunyi
7	Terdeteksi	Berbunyi
8	Terdeteksi	Berbunyi
9	Terdeteksi	Berbunyi
10	Terdeteksi	Berbunyi

I Made Yogaswara Dipta: Perancangan *Prototype* Sistem Pendeteksi...



Gambar 11: Pelaksanaan pengujian subsistem peringatan buzzer

4. Pengujian subsistem komunikasi *internet of things*

Pengujian subsistem komunikasi *internet of things* berfokus pada pengujian terhadap respon pengiriman notifikasi adanya penyusup ke aplikasi telegram. Pada skenario pengujian, dilakukan percobaan dengan menempatkan manusia yang bergerak di depan sensor PIR dengan jarak yang bervariasi. selanjutnya diamati respon aplikasi telegram terhadap hasil pembacaan sensor PIR ketika terdapat pergerakan manusia. Berdasarkan pengujian subsistem peringatan *buzzer* yang dilaksanakan, didapatkan hasil uji sesuai yang ditampilkan pada Tabel 8.

TABEL 8
HASIL PENGUJIAN SUBSISTEM PERINGATAN BUZZER

Jarak (cm)	Respon sensor PIR	Respon Telegram App
50	Terdeteksi	Notifikasi terkirim
100	Terdeteksi	Notifikasi terkirim
150	Terdeteksi	Notifikasi terkirim
200	Terdeteksi	Notifikasi terkirim
250	Terdeteksi	Notifikasi terkirim
300	Terdeteksi	Notifikasi terkirim
350	Terdeteksi	Notifikasi terkirim
400	Terdeteksi	Notifikasi terkirim
450	Terdeteksi	Notifikasi terkirim
500	Tidak terdeteksi	Tidak ada notifikasi



Gambar 12: Pelaksanaan pengujian subsistem komunikasi *internet of things*

5. Pengujian subsistem pengukur jarak

Pengujian subsistem pengukur jarak berfokus pada pengujian terhadap pembacaan jarak oleh sensor ultrasonik. Pada skenario pengujian, dilakukan percobaan dengan

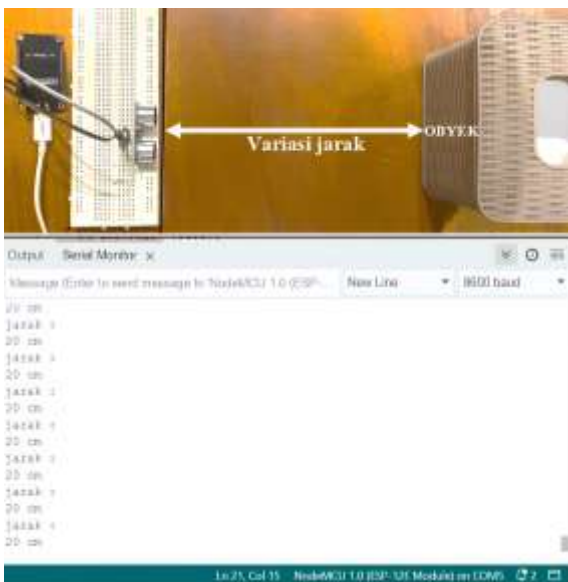
p-ISSN:1693 – 2951; e-ISSN: 2503-2372



menempatkan obyek di depan sensor ultrasonik dengan jarak yang bervariasi. Selanjutnya diamati hasil pembacaan jarak oleh sensor ultrasonik dibandingkan dengan jarak obyek aktual. Berdasarkan pengujian subsistem pengukur jarak dengan sensor ultrasonik, diperoleh hasil seperti yang ditunjukkan pada Tabel 9.

TABEL 9
HASIL PENGUJIAN SUBSISTEM PENGUKUR JARAK

Jarak sebenarnya (cm)	Jarak terukur oleh sensor PIR (cm)	Error (%)
10	10	0
20	20	0
30	30	0
40	40	0
50	50	0
60	61	1,67
70	69	1,42
80	80	0
90	90	0
100	99	1
Rata-rata penyimpangan		0,41



Gambar 13: Pelaksanaan pengujian subsistem pengukur jarak

6. Pengujian subsistem pengambilan gambar

Pengujian subsistem pengambilan gambar berfokus pada pengujian terhadap pengambilan oleh kamera ESP-32 dan pengiriman gambar ke aplikasi telegram. Pada skenario pengujian, dilakukan percobaan dengan memberikan perintah untuk mengambil gambar oleh kamera ESP-32. Selanjutnya diamati apakah kamera dapat mengirim gambar aplikasi telegram sesuai dengan perintah. Berdasarkan pengujian subsistem pengambilan gambar dengan ESP-32 cam, maka dapat ditampilkan hasil pengujian sesuai dengan Tabel 10.

TABEL 10
HASIL PENGUJIAN SUBSISTEM PENGAMBILAN GAMBAR

Percobaan	Perintah telegram	Respon telegram
1	/photo	Gambar terkirim
2	/photo	Gambar terkirim
3	/photo	Gambar terkirim
4	/photo	Gambar terkirim
5	/photo	Gambar terkirim



Gambar 14: Pelaksanaan pengujian subsistem pengambilan gambar

B. Hasil pengujian subsistem

Terdapat 3 (tiga) skenario untuk menguji keseluruhan sistem. Skenario pertama, seseorang memanjat dari sisi kiri pagar pembatas, dengan posisi sejajar dengan sensor ultrasonik-1 (bagian kiri) namun jauh dari sensor ultrasonik-3 (bagian kanan). Skenario kedua, seseorang memanjat dari sisi kanan pagar pembatas, dengan posisi sejajar dengan sensor ultrasonik-3 (bagian kanan) namun jauh dari sensor ultrasonik-1 (sisi kiri). Skenario ketiga, seseorang memanjat dari tengah pagar pembatas, dengan jarak orang tersebut ke sensor ultrasonik di sisi kanan dan kiri sama. Hasil pengujian skenario III ditunjukkan pada Tabel 10.

TABEL 10
TABEL CONFUSION MATRIX

No	Kondisi nyata	Status oleh PIDS			Klasifikasi		
		S-1	S-2	S-3	S-1	S-2	S-3
1	Ada	Ada	Tdk ada	Ada	TP	FP	TP
2	Ada	Ada	Ada	Ada	TP	TP	TP
3	Ada	Ada	Ada	Tdk ada	TP	TP	FP
4	Ada	Tdk ada	Ada	Tdk ada	FP	TP	FP
5	Ada	Ada	Ada	Tdk ada	TP	TP	TP
6	Ada	Ada	Ada	Tdk ada	TP	TP	FP
7	Ada	Ada	Tdk ada	Ada	TP	FP	TP
8	Ada	Tdk ada	Tdk ada	Ada	FP	FP	TP
9	Ada	Ada	Ada	Tdk ada	TP	TP	FP
10	Ada	Ada	Ada	Tdk ada	TP	TP	FP
11	Ada	Ada	Ada	Ada	TP	TP	TP
12	Ada	Ada	Ada	Ada	TP	TP	TP
13	Ada	Tdk ada	Tdk ada	Ada	FP	FP	TP
14	Ada	Ada	Ada	Ada	TP	TP	TP
15	Ada	Ada	Ada	Tdk ada	TP	TP	FP
16	Tdk ada	Ada	Ada	Tdk ada	FN	FN	TN
17	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN
18	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN
19	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN
20	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN
21	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN
22	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN
23	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN
24	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN
25	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN
26	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN
27	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN
28	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN
29	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN
30	Tdk ada	Tdk ada	Tdk ada	Tdk ada	TN	TN	TN

Keterangan:

S-1	: Skenario 1	TP	: True Positive
S-2	: Skenario 2	FP	: False Positive
S-3	: Skenario 3	TN	: True Negative
		FN	: False Negative

Skenario pengujian implementasi prototipe PIDS yang dirancang disajikan pada Gambar 14 – Gambar 19. Hasil perancangan prototipe PIDS dapat dilihat pada Gambar 20.



Gambar 20: Prototype PIDS



Gambar 14: Pengujian skenario dengan upaya memanjat pagar



Gambar 15: Pengujian skenario dengan upaya memanjat pagar



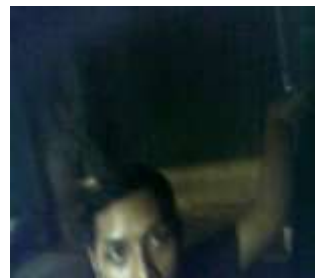
Gambar 16: Pengujian skenario dengan respon langsung pada aplikasi telegram



Gambar 17: Tampilan aplikasi telegram



Gambar 18: Tampilan foto yang diambil oleh ESP-32 Cam (malam hari)



Gambar 19: Tampilan foto yang diambil oleh ESP-32 Cam (malam hari)

Hasil perancangan *prototype* PIDS ditampilkan pada Gambar 20.

1.1 Analisis kinerja

Berdasarkan data yang diperoleh dari hasil pengujian skenario, maka selanjutnya dilakukan analisis kinerja dari *prototype* PIDS. Dalam analisis kinerja ini digunakan metode *confusion matrix* untuk mengukur akurasi dari sebuah eksperimen. Nilai yang diperoleh dengan metode *confusion matrix* berupa evaluasi sebagai berikut:

a. *Accuracy* merupakan presentase total *record* data yang diklasifikasikan benar (diprediksi secara benar sesuai kenyataannya oleh algoritma) dengan formula sebagai berikut:

$$Accuracy = \frac{True\ Positives\ (TP) + True\ Negatives\ (TN)}{Total\ data} \quad (1)$$

b. *Misclassification (error) rate* adalah presentase total *record* data yang diklasifikasikan salah (diprediksi secara salah oleh algoritma) dengan rumus sebagai berikut [35]:

$$Misclassification\ Rate = \frac{False\ Positives\ (FP) + False\ Negatives\ (FN)}{Total\ data} \quad (2)$$

Menurut Gorunesu [25], Akurasi diklasifikasikan dalam beberapa tingkatan yaitu:

- Akurasi sebesar 0.90 – 1.00 = *Excellent classification*
- Akurasi sebesar 0.80 – 0.90 = *Good classification*
- Akurasi sebesar 0.70 – 0.80 = *Fair classification*
- Akurasi sebesar 0.60 – 0.70 = *Poor classification*
- Akurasi sebesar 0.50 – 0.60 = *Failure*

Berdasarkan persamaan (1) dan (2) maka dapat dikalkulasi nilai *accuracy* dan *misclassification (error) rate*, dimana hasil perhitungan disajikan pada Tabel 11.

TABEL 11.
HASIL ANALISIS KINERJA

Parameter	Skenario I	Skenario II	Skenario III
Jumlah True positive (TP)	12	11	9
Jumlah False positive (FN)	1	1	0
Jumlah False positive (FP)	3	4	6
Jumlah True Negative (TN)	14	14	15
Jumlah sampel	30	30	30
Nilai <i>accuracy</i>	86.67%	83.33%	80.00%
<i>Misclassification (error) rate</i>	13.33%	16.67%	20.00%
Rata-rata <i>accuracy</i>	83.33%		
Rata-rata <i>misclassification (error) rate</i>	16.67%		

Berdasarkan analisis kinerja dari hasil pengujian skenario, maka dapat diketahui bahwa pada skenario I dimana



seseorang memanjat dari sisi kanan pagar, dengan posisi berdekatan dengan sensor ultrasonik-3 (bagian kanan) namun jauh dari sensor ultrasonik-1 (bagian kiri), diperoleh nilai akurasi sebesar 86.67% yang dapat dikategorikan sebagai *good classification*. Pada skenario II dimana seseorang memanjat dari sisi kanan pagar, dengan posisi berdekatan dengan sensor ultrasonik-3 (bagian kanan) namun jauh dari sensor ultrasonik-1 (bagian kiri), dapat diperoleh nilai akurasi sebesar 83.33% yang dapat diklasifikasikan sebagai *good classification*. Sementara itu, untuk skenario III dimana seseorang memanjat dari bagian tengah pagar, dengan jarak orang ke sensor ultrasonik pada sisi kanan dan sisi kiri adalah sama, maka didapatkan nilai akurasi sebesar 80.00% yang dapat dikategorikan sebagai *good classification*. Dari 3 (tiga) skenario yang diujikan, skenario III memiliki nilai akurasi terendah. Berdasarkan pengamatan ketika dilakukan percobaan, hal ini disebabkan oleh orang yang memanjat di bagian tengah pagar tidak terdeteksi dengan baik oleh sensor ultrasonik karena posisi sudut kemiringan sensor belum optimal mendeteksi adanya obyek. Berdasarkan analisis kinerja, secara umum dapat dinyatakan bahwa *prototype* sistem pendeteksi penyusup perimeter yang dirancang memiliki akurasi yang baik/*good classification* (83.33%).

IV. KESIMPULAN

Prototype Sistem Pendeteksi Penyusup Perimeter (*Perimeter Intruder Detection System/PIDS*) berbasis *Internet of Things* telah dirancang dengan menggunakan perpaduan sensor ultrasonik, sensor PIR, kamera ESP-32, Node MCU, relay, dan *buzzer*. Logika fuzzy digunakan untuk memetakan ruang *input* (dekat, sedang, jauh) ke dalam ruang *output* (ada penyusup, tidak ada penyusup). Pengujian dari *prototype* PIDS ini terdiri atas pengujian subsistem serta pengujian skenario untuk seluruh sistem. Kinerja dari perangkat dianalisis dengan metode *confusion matrix* dan dapat dinyatakan bahwa *prototype* sistem pendeteksi penyusup perimeter yang dirancang memiliki akurasi yang baik/*good classification* (83.33%).

REFERENSI

- [1] Peraturan Menteri Perhubungan Republik Indonesia Nomor: PM 51 Tahun 2020 tentang Keamanan Penerbangan Nasional
- [2] Amanda Nurma Hariyanti, Satiti Utami, Herman Susanto. *Kajian Pengamanan Perimeter Dalam Menunjang Keamanan Penerbangan Di Bandar Udara Internasional Adi Soemarmo-Surakarta*. Jurnal Ilmiah Aviasi Langit Biru Vol. 12 No.3 Oktober 2019 Hal 1 : 178
- [3] Keputusan Direktur Jenderal Perhubungan Udara Nomor KP 138 Tahun 2018 tentang Sertifikasi Peralatan Keamanan
- [4] Rinaldi. 2022. Materi ITS : Indoktrinasi Pengenalan Fasilitas Keamanan Penerbangan. Jakarta: Kementerian Perhubungan RI.
- [5] Xie Z, Qin Y. High-speed railway perimeter intrusion detection approach based on Internet of Things. *Advances in Mechanical Engineering*. 2019;11(2). doi:10.1177/1687814018821511.
- [6] Hoang ML. Smart Drone Surveillance System Based on AI and on IoT Communication in Case of Intrusion and Fire Accident. *Drones*. 2023; 7(12):694. <https://doi.org/10.3390/drones7120694>.
- [7] Rambabu, Kalathiripi. (2019). IoT Based Human Intrusion Detection System using Lab View. *International Journal of Innovative Technology and Exploring Engineering*. 8. 10.35940/ijitee.F1115.0486S419.
- [8] Seung Hyun Kim, Su Chang Lim, Do Yeon Kim, Intelligent intrusion detection system featuring a virtual fence, active intruder detection, classification, tracking, and action recognition, *Annals of Nuclear Energy*, Volume 112, 2018, Pages 845-855, ISSN 0306-4549, <https://doi.org/10.1016/j.anucene.2017.11.026>.
- [9] P. Shirin Saleem, A. Sushanand, J. A. Renji, M. Aman, D. James and K. S. Lakshmi, "AI-Empowered Intruder Alert System for Enhanced Security Surveillance," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 1-8, doi: 10.1109/ICACRS58579.2023.10404156.
- [10] [N. Chandra and S. P. Panda, "A Human Intruder Detection System for Restricted Sensitive Areas," 2021 2nd International Conference on Range Technology (ICORT), Chandipur, Balasore, India, 2021, pp. 1-4, doi: 10.1109/ICORT52730.2021.9582099.
- [11] Prabu and P. Sudhakar, "Design and Implementation of an Automated Control System for Anomaly Detection Using an Enhanced Intrusion Detection System," 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, India, 2022, pp. 1-7, doi: 10.1109/ICSTCEE56972.2022.10100003.
- [12] D. Arjun, P. Indukala and K. A. U. Menon, "Integrated Multi-sensor framework for Intruder Detection in Flat Border Area," 2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC), Chennai, India, 2019, pp. 557-562, doi: 10.1109/ICPEDC47771.2019.9036577.
- [13] D. Arjun, P. K. Indukala and K. A. Unnikrishna Menon, "PANCHENDRIYA: A Multi-sensing framework through Wireless Sensor Networks for Advanced Border Surveillance and Human Intruder Detection," 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2019, pp. 295-298, doi: 10.1109/ICCES45898.2019.9002161.
- [14] Peijun Zhao, Chris Xiaoxuan Lu, Jianan Wang, Changhao Chen, Wei Wang, Niki Trigoni, Andrew Markham, Human tracking and identification through a millimeter wave radar, *Ad Hoc Networks*, Volume 116, 2021, 102475, ISSN 1570-8705, <https://doi.org/10.1016/j.adhoc.2021.102475>.
- [15] S. Yasukawa and M. Kim, "Intruder Detection Using Radio Wave Propagation Characteristics," 2018 IEEE International Conference on Consumer Electronics - Asia (ICCE-Asia), Jeju, Korea (South), 2018, pp. 206-212, doi: 10.1109/ICCE-ASIA.2018.8552128.
- [16] Almonfrey D, do Carmo AP, de Queiroz FM, Picoreti R, Vassallo RF, Salles EOT. A flexible human detection service suitable for Intelligent Spaces based on a multi-camera network. *International Journal of Distributed Sensor Networks*. 2018;14(3). doi:10.1177/1550147718763550.
- [17] Sri Yulianto J.P., Indrastanti R.W., Martha Oktriani. Decision Support Applications Using Fuzzy Logic (Case Study: Determination of Computer Specifications for a Complete Computer Package). *Journal of Informatics*, Vol.4, No. 2, December 2008: 159 – 173
- [18] Harahap, Siti Dewi Dayanti. 2019. "Automatic Door Design Using Fuzzy Logic Control Method." *Jurnal Pelita Informatika*, Vol.7, No.4, 579-582.
- [19] N. K. Sabat, U. C. Pati, B. R. Senapati and S. K. Das, "An IoT-Secnet for Region Based Human Detection Using PIR Sensors and FRED Cloud," 2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP), Chennai, India, 2019, pp. 1-4, doi: 10.1109/ICESIP46348.2019.8938286.
- [20] Abdullah, Cholish, Moh. Zainul Haq. Utilization of IoT (Internet of Things) in Monitoring Smoke Density Levels and Camera Tracking Control. *Scientific Journal of Electrical Engineering Education*, Vol.5, No.1, February 2021 H.86
- [21] China factory anti climb electric fence energizer and alarm for home and garden URL: https://www.alibaba.com/product-detail/China-factory-anti-climb-electric-fence_60756687786.html?spm=a2700.galleryofferlist.normal_offer.d_title.f0ca44bdklayqe
- [22] Putra, I., Sukardarmika, G., & Sastra, N. (2023). Perankingan Dosen Berbasis Aktifitas Forum Moodle Menggunakan Metode Fuzzy Tsukamoto. *Majalah Ilmiah Teknologi Elektro*, 22(1), 63-70. doi:10.24843/MITE.2023.v22i01.P08
- [23] Sutikno, T., Susanto, D., & Purnama, H. (2023). Sistem Monitoring Debit Air Berbasis Internet of Things pada Saluran Air. *Majalah Ilmiah Teknologi Elektro*, 22(2), 159-164. doi:10.24843/MITE.2023.v22i02.P01
- [24] Rima Tamara Aldisa, Sechan Alfaria. Sistem Pendeteksi Keamanan Ruang "Smart Security" Dengan Metode Fuzzy Logic Menggunakan Sensor PIR Berbasis Internet of Things (IoT). Volume 4, Nomor 1, September 2022. Hal: 176-183
- [25] Gorunescu, F. (2011). Data Mining: Concepts, Models and Techniques. *Data mining - Concepts, Models and Technique*. <https://doi.org/10.1007/978-3-642-19721-5>.