JOURNAL
INFORMATION & COMPUTER

Vol. 4, No.2, July 2026

JICOM

E-ISSN: 3026-4197
P-ISSN: 3031-2779

sinta 4
Science and Technology Index

Jicom : Journal Information & Computer
Volume 4, Nomor 2, July 2026
DOI: 10.32493/jicomisc.v2i1.37666

E-ISSN: 3026-4197
P-ISSN: 3031-2779

Journal Information & Computer
Volume 4, Nomor 2, July 2026

Available online at http://openjournal.unpam.ac.id/index.php/jisc

Alamat Redaksi
Universitas Pamulang – PSDKU Kampus Kota Serang
Fakultas Ilmu Komputer
Jl. Lintas Serang - Jakarta Kampung Limandang, Kelurahan Kelodran, Kecamatan Walantaka Kota Serang Banten
E-mail: ojsjicom@unpam.ac.id

Penerbitan:
Terbit 2 kali dalam satu tahun, setiap bulan January dan July

Penerbit:
Program Studi Sistem Komputer Universitas Pamulang PSDKU Kampus Kota Serang
https://openjournal.unpam.ac.id/index.php/jisc

Jicom : Journal Information & Computer
Volume 4, Nomor 2, July 2026
DOI: 10.32493/jicomisc.v2i1.37666

E-ISSN: 3026-4197
P-ISSN: 3031-2779

Dewan Redaksi

JICOM *Journal Information & Computer* adalah jurnal ilmiah yang diterbitkan 2 edisi dalam setahun yaitu pada bulan January dan July oleh Program Studi Sistem Komputer Universitas Pamulang-PSDKU Kampus Kota Serang. Terbit sejak bulan July tahun 2023. Fokus kajian jurnal ini adalah berkaitan dengan penelitian pada bidang Ilmu Komputer. Lingkup jurnal JICOM meliputi penelitian Sistem Informasi, *Internet of Things*, *Artificial Intelegence*, Data Mining dan Ilmu ilmu komputer lainnya

Alamat Redaksi: Jl. Lintas Serang - Jakarta Kampung Limandang, Kelurahan Kelodran, Kecamatan Walantaka Kota Serang Banten
Telp/WA. +6281818993063

e-mail: ojsjicom@unpam.ac.id

Mohon dibaca panduan dengan baik. Penulis yang ingin menyerahkan artikel ke JICOM, harus mematuhi panduan penulisan. Jika artikel yang dikirim tidak sesuai atau ditulis dalam format yang berbeda dengan panduan, maka akan **DITOLAK** oleh editor sebelum ditinjau lebih lanjut. Para editor hanya menerima artikel yang sesuai dengan format yang telah ditetapkan. Artikel ditulis dalam bahasa Indonesia.

Jicom : Journal Information & Computer
Volume 4, Nomor 2, July 2026
DOI: 10.32493/jicomisc.v2i1.37666
E-ISSN: 3026-4197
P-ISSN: 3031-2779

Pengantar Redaksi

Assalamu'alaikum Wr. Wb.

Puji syukur kami panjatkan kehadirat Allah SWT, yang telah melimpahkan Rahmat, Taufiq serta Hidayah-Nya sehingga JICOM Journal Information & Computer sebagai jurnal ilmiah Program Studi Sistem Komputer Univesitas Pamulang-PSDKU Kampus Kota Serang dapat terbit pada bulan **July 2026**. Kami terus mendorong segenap Civitas Akademika untuk benar-benar memanfaatkan JICOM Journal Information & Computer ini sebagai sarana pembelajaran bagi semua yang terlibat dalam penerbitan jurnal ini secara berkala. Selanjutnya kami dari Tim JICOM Journal Information & Computer mengucapkan banyak-banyak terima kasih kepada instansi-instansi *(Universitas Utpadaka Swastika, Universitas Multi Data Palembang, Universitas Islam Negeri Sultan Syarif Kasim Riau, Universitas Budi Luhur, dan Universitas Pamulang)* yang telah mempublikasikan artikalnya pada OJS kami.

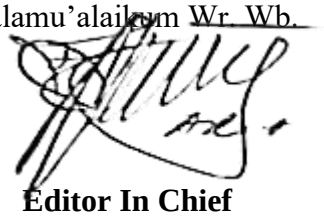
JICOM Journal Information & Computer adalah jurnal ilmiah yang diterbitkan 2 edisi dalam setahun (January & July) oleh Program Studi Sistem Komputer Univesitas Pamulang-PSDKU Kampus Kota Serang. Terbit sejak bulan **July tahun 2023**. Fokus kajian jurnal ini adalah berkaitan dengan penelitian pada bidang Komputer. JICOM Journal Information & Computer meliputi penelitian ***Sistem Informasi, Internet of Things, Artificial Intelegence, Data Mining dan Ilmu-ilmu komputer lainya.***

Mohon dibaca panduan dengan baik. Penulis yang ingin menyerahkan artikel JICOM Journal Information & Computer, harus mematuhi panduan penulisan. Jika artikel yang dikirim tidak sesuai atau ditulis dalam format yang berbeda dengan panduan, maka akan **Ditolak** oleh editor sebelum ditinjau lebih lanjut. Para editor hanya menerima artikel yang sesuai dengan format yang telah ditetapkan. Artikel ditulis dalam bahasa indonesia. Kepada segenap penyumbang karya tulis pada terbitan kali ini redaksi memberikan apresiasi dan mengucapkan terima kasih.

E-ISSN: 3026-4197
P-ISSN: 3031-2779

Semoga penerbitan JICOM Journal Information & Computer edisi ini memberi manfaat dan dari redaksi mengucapkan selamat membaca.

Wassalamu'alaikum Wr. Wb.



Editor In Chief

Jicom : Journal Information & Computer
Volume 4, Nomor 2, July 2026
DOI: 10.32493/jicomisc.v2i1.37666
E-ISSN: 3026-4197
P-ISSN: 3031-2779

Daftar Isi

Jicom : Journal Information & Computer
Volume 4, Nomor 2, Juli 2026, hlm. 62-67
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Perancangan Sistem Otomatisasi Berbasis Id Card Dan Internet Of Things (Iot) Pada Pintu Kamar Kost Menggunakan Mikrokontroller Esp32

Febiyana Firdaus*[1], Agus Suhendi[2]
[1,2)]Program Studi Sistem Komputer, Fakultas Ilmu Komputer, Universitas Pamulang
Email: *[1]febbyyanafirdaus5549@gmail.com, [2]dosen10007@unpam.ac.id

(Naskah masuk: *7 Mei 2026*, diterima untuk diterbitkan: *31 Juli 2026*)

Abstrak: *Di era teknologi modern, sistem keamanan yang efektif dan mudah digunakan semakin dibutuhkan, terutama untuk properti sewaan seperti kamar kost. Tujuan penelitian ini adalah untuk mengembangkan dan merancang sistem otomasi pintu persewaan berbasis ID card dan Internet of Things (IoT) yang menggunakan mikrokontroler ESP32 di lingkungan Secang. Sistem ini terdiri dari beberapa komponen utama, yaitu mikrokontroler ESP32 sebagai pusat kendali, reader RFID untuk membaca ID card, dan modul Wi-Fi untuk menghubungkan IoT. Hanya penyewa yang telah mendaftarkan kartu identitasnya di sistem yang dapat membuka pintu persewaan. Platform IoT mencatat dan memantau akses secara real-time, memungkinkan pemilik rumah melacak aktivitas masuk dan keluar. Penelitian ini menggunakan pendekatan penelitian dan pengembangan (R&D) model prototipe untuk membangun sistem dan alat pengunci pintu kamar otomatis berbasis Kartu Resmi. Sudah jelas bahwa penerapan sistem ini memiliki hasil yang baik. Keandalan dan keamanan diuji dalam berbagai situasi. Sistem akan mengenali identitas individu dan secara otomatis membuka pintu. Selain itu, kemampuan pemantauan berbasis IoT memungkinkan pemilik menerima peringatan jika terjadi akses ilegal. Hasil penelitian menunjukkan bahwa ID card yang berfungsi dengan sistem otomasi pintu berbasis ESP32 dan IoT dapat berfungsi sebagai solusi yang efektif untuk meningkatkan keamanan dan efisiensi di tempat tinggal sewa*

Kata Kunci – Sistem Otomatisasi, *RFID ID Card*, *Internet of Things* (IoT), Pintu Otomatis, ESP32, Rumah Pintar

Abstract: *In the modern technological era, effective and easy-to-use security systems are increasingly needed, especially for rental properties such as boarding houses. The purpose of this research is to develop and design an ID card-based rental door automation system and the Internet of Things (IoT) using an ESP32 microcontroller in the Secang environment. This system consists of several main components, namely an ESP32 microcontroller as a control center, an RFID reader to read ID cards, and a Wi-Fi module to connect to the IoT. Only tenants who have registered their ID cards in the system can open the rental door. The IoT platform records and monitors access in real-time, allowing homeowners to track entry and exit activities. This research uses a prototype model research and development (R&D) approach to build an automatic room door locking system and device based on an Authorized Card. It is clear that the implementation of this system has good results. Reliability and security are tested in various situations. The system will recognize individual identities and automatically open the door. In addition, IoT-based monitoring capabilities allow owners to receive alerts in the event of unauthorized access. The results of the study show that ID cards that function with ESP32 and IoT-based door automation systems can serve as an effective solution to improve security and efficiency in rental residences.*

Keywords *– Automation System, RFID ID Card, Internet of Things (IoT), Automatic Door, ESP32, Smart Home*

1. PENDAHULUAN

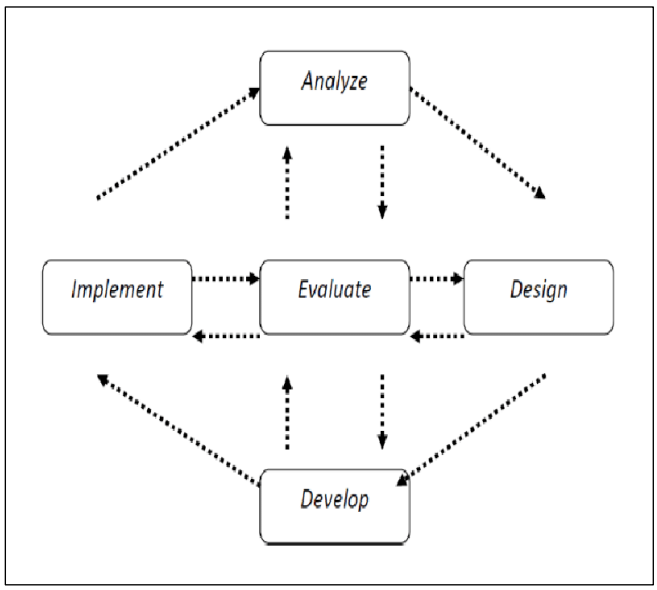
Keamanan merupakan aspek penting dalam hunian, terutama pada kamar kost yang umumnya masih menggunakan sistem kunci konvensional. Sistem tersebut memiliki berbagai kelemahan seperti risiko kehilangan kunci, pencurian, serta tidak adanya pemantauan jarak jauh. Dengan berkembangnya teknologi Internet of Things (IoT), sistem keamanan dapat ditingkatkan melalui integrasi perangkat pintar [1]. Penggunaan RFID sebagai identifikasi pengguna dan ESP32 sebagai pengendali memungkinkan sistem bekerja secara otomatis dan terhubung ke internet. Penelitian ini bertujuan untuk merancang sistem keamanan pintu otomatis berbasis ID Card dan IoT yang mampu meningkatkan keamanan serta memberikan kemudahan dalam monitoring akses secara real-time [2].

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan *Research and Development* (R&D) dengan model prototipe untuk merancang sistem otomatisasi pintu kamar kost yang mengintegrasikan teknologi *Internet of Things* (IoT) dan mikrokontroler ESP32 [4].

2.1. Analisa dan Arsitektur Tahapan

Analisis sistem dilakukan untuk mengatasi kelemahan kunci mekanis konvensional yang rentan terhadap pencurian dan sulit dipantau, sehingga diajukan sistem cerdas yang mampu melakukan autentikasi otomatis dan pemantauan jarak jauh. Arsitektur sistem berpusat pada mikrokontroler ESP32 yang terhubung dengan pembaca RFID RC522 untuk identifikasi ID card, keypad matriks sebagai akses cadangan, serta aktuator micro servo untuk menggerakkan mekanisme pengunci pintu [5].



Gambar 1 Metode Penelitian R&D

2.2. Metode Penyelesaian Masalah

Metode penyelesaian masalah dalam penelitian ini dilakukan melalui pendekatan *Research and Development* (R&D) dengan menggunakan model pengembangan prototipe untuk menciptakan sistem keamanan yang lebih cerdas [5]. Proses diawali dengan tahap analisis untuk mengidentifikasi kelemahan kunci manual yang kemudian diterjemahkan ke dalam perancangan arsitektur sistem berbasis mikrokontroler ESP32 sebagai pusat kendali. Selanjutnya, dilakukan integrasi perangkat keras seperti sensor RFID RC522 untuk autentikasi kartu dan *micro servo* sebagai penggerak kunci otomatis [6]. Penyelesaian masalah diperkuat dengan pengembangan perangkat lunak pada Arduino IDE yang memungkinkan sistem terhubung ke jaringan internet melalui fitur IoT untuk mengirimkan notifikasi *real-time* ke platform Telegram Bot. Tahap akhir melibatkan pengujian fungsionalitas untuk memastikan bahwa sistem mampu memberikan peringatan otomatis terhadap akses ilegal dan menyediakan log aktivitas yang akurat bagi pemilik kost [7].

2.3. Implementasi Sistem

Implementasi perangkat lunak dilakukan menggunakan Arduino IDE dengan logika pemrograman *IF-ELSE* untuk memvalidasi identitas kartu; jika data sesuai, ESP32 akan memerintahkan servo membuka pintu dan mengirimkan notifikasi *real-time* ke pemilik melalui platform Telegram Bot [8]. Pengujian sistem menunjukkan bahwa prototipe ini efektif meningkatkan keamanan melalui fitur peringatan otomatis jika terjadi akses ilegal, serta memberikan efisiensi manajemen hunian dengan pencatatan log aktivitas yang dapat dipantau secara daring [9].

2.4. Pengujian dan Hasil

Penelitian ini menunjukkan bahwa prototipe sistem otomatisasi pintu kamar kost berbasis IoT berhasil meningkatkan standar keamanan dan efisiensi manajemen hunian [10]. Penggunaan mikrokontroler ESP32 yang terintegrasi dengan sensor RFID RC522 dan *keypad* terbukti efektif dalam memvalidasi akses pengguna secara akurat, sehingga meminimalisir risiko penggunaan kunci ilegal [11]. Selain itu, penerapan teknologi *Internet of Things* melalui platform Telegram Bot memungkinkan pemilik kost untuk menerima notifikasi *real-time* dan memantau log aktivitas pintu secara daring tanpa batasan jarak. Dengan demikian, sistem ini memberikan solusi keamanan yang lebih aktif, transparan, dan responsif dibandingkan dengan sistem kunci mekanis konvensional [12].

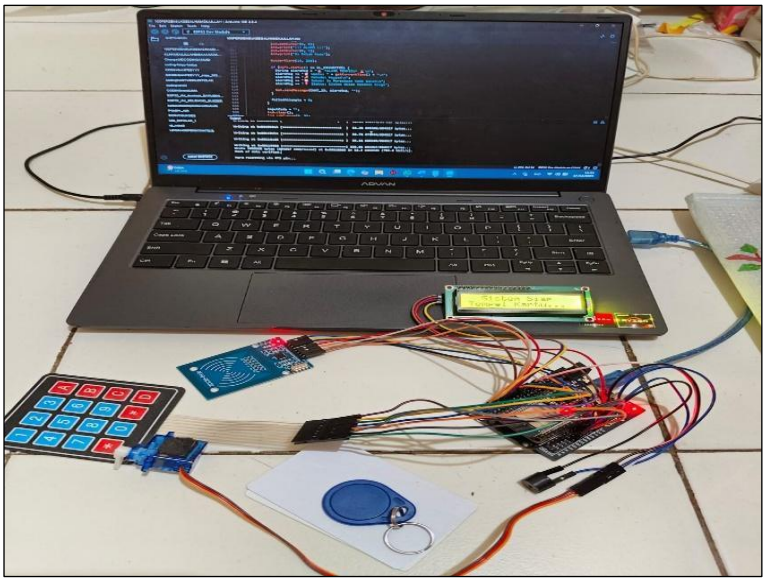
3. HASIL DAN PEMBAHASAN

3.1. Hasil

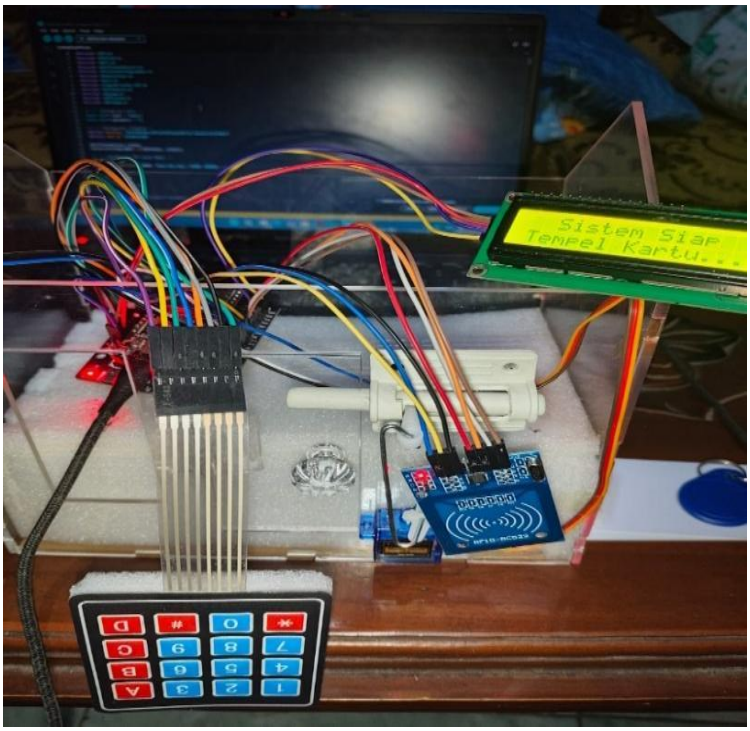
Hasil penelitian menunjukkan bahwa sistem otomatisasi pintu berbasis ID Card dan IoT menggunakan ESP32 dapat bekerja dengan baik dalam membaca kartu, memverifikasi akses, membuka pintu secara otomatis, serta mengirimkan notifikasi secara real-time, sehingga mampu meningkatkan keamanan dan kemudahan dalam pengelolaan akses kamar kost [13].

3.1.1 Gambar Hasil Perancangan dan Uji Coba

Perancangan *Hardware* pada sistem ini bertujuan untuk membangun Sistem Otomatisasi Pintu Kamar Kost Berbasis ID *Card* dan *Internet of Things* (IoT) menggunakan mikrokontroler ESP32. Untuk menjalankan ESP32 beserta seluruh modul pendukungnya, yang dapat diperoleh melalui adaptor USB atau sumber daya lain sesuai spesifikasi ESP32 [14].



Gambar 2 Hasil Perakitan Alat



Gambar 3 Hasil Uji Coba Alat

Pada tahap ini dilakukan Hasil Pengujian Telegram Bot sebagai bagian dari sistem IoT untuk memastikan bahwa fitur notifikasi dapat berjalan dengan baik. Pengujian ini bertujuan untuk mengetahui apakah sistem mampu mengirimkan informasi aktivitas akses pintu secara real-time, baik saat akses diterima maupun ditolak, sehingga pengguna dapat memantau kondisi sistem secara langsung melalui aplikasi Telegram.

Gambar 4 Hasil Uji Coba pada Telegram Bot

3.1.2 Tabel Hasil Pengujian Sistem

Sistem diuji dengan menempelkan kartu RFID yang telah didaftarkan pada basis data mikrokontroler. Ketika kartu terdeteksi, ESP32 memverifikasi UID dan menginstruksikan Servo untuk berputar 90° guna membuka kunci. Secara bersamaan, notifikasi dikirimkan ke Telegram Bot pemilik.

Tabel 1 Menampilkan Hasil Pengujian Sistem

No	Waktu	Metode Akses	Identitas/ UID Kartu	Status Akses	Status Micro Servo	Kesesuaian Logika (Ya/Tidak)
1	18:18	RFID (*Card*) Sah	BF7A661F (Zahra Ainun)	Akses Diterima	Berputar 90° (Buka)	Ya
2	18.20	RFID (*Card*) Sah	D333D507 (Ningsih)	Akses Diterima	Berputar 90° (Buka)	Ya
3	18.22	RFID (Tag&*Card*) Ilegal	DA3E7A00 (3 Kali Gagal)	Alarm Terpicu	Tertutup 90°	Ya
4	18.23	Keypad Code	Pin Benar	Akses Diterima	Berputar 90° (Buka)	Ya

3.2 Pembahasan

Pembahasan ini berfokus pada penggabungan sistem keamanan fisik dan pemantauan berbasis digital yang dapat berjalan bersama-sama melalui jaringan internet. Pengujian menunjukkan bahwa penggunaan ESP32 sebagai pusat kendali sangat efektif karena kecepatan proses data yang stabil dan konektivitas Wi-Fi bawaan yang andal. Ini memungkinkan pengiriman notifikasi ke Telegram Bot dalam beberapa detik setelah sensor RFID dipicu. Namun, sensor MFRC522 harus ditempatkan dengan tepat di atas permukaan pintu agar tidak terhalang oleh material yang terlalu tebal atau logam yang dapat mengganggu gelombang radio RFID, karena jarak baca optimalnya pada rentang 1 hingga 3 cm menunjukkan bahwa sistem ini memiliki sensitivitas yang cukup tinggi untuk penggunaan sehari-hari.

Selain fungsi pembukaan pintu, Pembahasan ini juga membahas aspek keamanan pencegahan melalui fitur peringatan akses ilegal. Ketika sistem menemukan kartu UID yang tidak ada dalam basis data mikrokontroler, aktuator servo tidak akan membuka kunci. Sebaliknya, sistem secara otomatis memicu alarm dan mengirimkan pesan peringatan khusus ke ponsel pemilik kost. Hal ini menunjukkan bahwa sistem tidak hanya berfungsi sebagai pengganti kunci mekanis tetapi juga sebagai alat pengawasan aktif yang memberikan rasa aman yang lebih besar bagi pemilik rumah. Keberhasilan penggunaan log aktivitas yang mencatat nama pengguna dan waktu akses membuktikan bahwa teknologi IoT dapat menyelesaikan masalah transparansi akses yang selama ini menjadi masalah utama pada sistem penguncian konvensional di kawasan hunian kost.

4. KESIMPULAN

Penelitian ini berhasil mengembangkan prototipe sistem *smart door lock* berbasis IoT menggunakan ESP32 yang mampu mengatur akses pintu kamar kost secara otomatis melalui ID *Card* dan keypad,

menggerakkan kunci dengan micro servo, serta menyediakan monitoring dan notifikasi *real-time* melalui Telegram, sehingga meningkatkan keamanan dengan deteksi akses ilegal dan tampilan status melalui LCD

DAFTAR PUSTAKA

[1] G. Eason, B. Noble, dan I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, hal. 529-551, April 1955.

[2] S. Andrean, S. Y. Putri, et al., "No title," n.d.

[3] F. Badri, H. Afifah, A. M. Jannah, M. Nafis, N. Murom, dan A. Andhyka, "Simulasi rancang bangun palang pintu otomatis berbasis RFID (Radio Frequency Identification)," *JISTI: Jurnal Ilmiah Terapan, Sains dan Teknologi*, vol. 1, no. 3, pp. 137–143, 2023.

[4] R. Bima, "Analisis RFID Reader MFRC522 pada sistem informasi lokasi meja pelanggan Kopi Kenangan," *Jurnal Komputer Teknologi Informasi dan Sistem Informasi (JUKTISI)*, vol. 2, no. 1, pp. 248–256, 2023.

[5] M. Fauza dan M. A. Muthalib, "Sistem pengaman pintu otomatis menggunakan sensor Radio Frequency Identification (RFID) berbasis Arduino Uno," *Jurnal Energi Elektrik*, vol. 11, no. 1, p. 30, 2022.

[6] I. G. P. Wirajaya, "Penerapan rancang bangun pintu kunci menggunakan sensor Radio Frequency Identification (RFID)," Politeknik Negeri Bali, 2023.

[7] M. Hipotesis, M. Nur, R. P. Junita, et al., "JOLR," vol. 1, no. 2, pp. 810–820, 2025.

[8] K. Lesmana, "Prototipe penggunaan motor servo untuk dispenser otomatis berbasis Arduino dan sensor HC-SR04," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 2, pp. 16–22, 2025.

[9] A. Martani, J. Junaedy, dan M. Gogasa, "Prototipe robot penanam benih jagung berbasis ESP32-CAM," *Journal of System and Computer Engineering (JSCE)*, vol. 4, no. 2, pp. 145–153, 2023.

[10] Y. A. Muhammad dan R. A. Permana, "Prototipe monitoring lampu jalan otomatis menggunakan mikrokontroler ESP32 dan API Bot Telegram," *Jurnal Teknik Informatika STMIK Antar Bangsa*, vol. 9, no. 2, pp. 57–62, 2023.

[11] P. Pengujian, "Hipotesis penelitian dalam statistik manajemen pendidikan: Konsep," vol. 1, pp. 425–433, 2025.

[12] Y. R. Putung, H. S. Langi, S. Kasenda, dan T. J. Wungkana, "Perancangan sistem akses masuk ruangan berbasis Internet of Things (IoT) dengan kartu tanda penduduk (KTP) elektronik," vol. 4, no. 1, pp. 63–70, 2025.

[13] A. Rahayu, "Tahapan," *Jurnal Pendidikan dan Pembelajaran*, vol. 4, no. 3, pp. 459–470, 2025.

[14] D. A. Ramadini et al., "Pintu menggunakan IoT berbasis E-KTP," vol. 13, no. 1, 2025.

[15] H. Saputri, U. Kusnaedi, dan Y. Asmana, "Pengaruh sistem informasi akuntansi terhadap kualitas laporan keuangan perusahaan jasa di Jakarta Utara," vol. 1, no. 4, pp. 102–109, 2023.

[16] A. Selay et al., "Karimah Tauhid," vol. 1, no. 6, pp. 861–862, 2022.

[17] S. Sutarti, T. Triyatna, dan S. Ardiansyah, "Prototype sistem absensi siswa/i dengan menggunakan sensor RFID berbasis Arduino Uno," *PROSISKO*, vol. 9, no. 1, pp. 76–85, 2022.

[18] V. N. Tahun et al., "Jurnal Al Ulum LPPM Universitas Al Washliyah Medan," vol. 14, no. 1, 2026.

[19] R. Tho, A. Firdaus, S. Sabila, dan Y. Yuniarsih, "Strategi target pasar pada produk custom acrylic di Kota Bandung," vol. 3, no. 1, 2023.

[20] U. M. Tyas et al., "Implementasi aplikasi Arduino IDE pada mata kuliah sistem digital," vol. 1, Apr. 2023

Jicom : Journal Information & Computer
Volume 4, Nomor 2, Juli 2026, hlm. 68-73
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Klasifikasi Pemilihan Buah Cabai Menggunakan Traction Control System Berbasis Internet Of Things (*IoT*)

Ranti Imawati*[1], Asep Suryadi[2],
[1,2)]Program Studi Sistem Komputer, Fakultas Ilmu Komputer,Universitas Pamulang
Email: *[1]rantiimawati2@gmail.com,[2] dosen10008@unpam.ac.id

(Naskah masuk: *8 Juni 2026*, diterima untuk diterbitkan: *31 Juli 2026*)

Abstrak: *Cabai merupakan produk pertanian yang memiliki nilai komersial tinggi, terutama karena kualitas dan kematangannya. Warna cabai merupakan indikator paling penting untuk menentukan kematangan dan daya jual. Namun ada batasan dalam menyortir cabai dengan tangan. Misalnya, membutuhkan waktu, memiliki tingkat akurasi yang bervariasi, dan bergantung pada usaha manusia. Oleh karena itu, penelitian ini bertujuan untuk merancang dan mengembangkan prototipe sistem sortasi dan klasifikasi cabai berbasis warna dengan menggabungkan sensor TCS3200 dengan Internet of Things (IoT). Sensor TCS3200 digunakan untuk mendeteksi warna cabai. Warna-warna tersebut kemudian diproses oleh mikrokontroler untuk memilah cabai ke dalam kategori hijau, merah, dan kuning. Data hasil klasifikasi dikirimkan dan ditransmisikan secara real time melalui platform IoT, memungkinkan pemantauan jarak jauh dan analisis data yang lebih efektif. Sistem ini juga dilengkapi dengan aktuator mekanis untuk memilah cabai secara otomatis. Pengujian dilakukan untuk kedalaman sensor dalam mendeteksi warna dan efisiensi sistem dalam proses penyortiran. Hasil percobaan menunjukkan bahwa sistem dapat melakukan klasifikasi dengan akurasi tinggi dan meningkatkan efisiensi penyortiran dibandingkan dengan metode manual. Teknologi ini dirancang untuk membuat proses penyortiran cabai lebih cepat dan akurat serta dapat diterapkan dalam skala industri untuk meningkatkan produktivitas dan kualitas hasil pertanian..*

Kata Kunci *– Klasifikasi Cabai; TCS3200; Internet of Things; Penyortiran Otomatis; Pertanian cerdas.*

Abstract: *Chili peppers are an agricultural product with high commercial value, primarily due to their quality and ripeness. Chili color is the most important indicator for determining ripeness and marketability. However, there are limitations in sorting chili peppers by hand. For example, it is time-consuming, has varying degrees of accuracy, and relies on human effort. Therefore, this study aims to design and develop a prototype of a color-based chili sorting and classification system by combining the TCS3200 sensor with the Internet of Things (IoT). The TCS3200 sensor is used to detect the color of chili peppers. These colors are then processed by a microcontroller to sort chili peppers into green, red, and yellow categories. Classification data is sent and transmitted in real time through an IoT platform, enabling remote monitoring and more effective data analysis. The system is also equipped with mechanical actuators for automatic chili sorting. Tests were conducted to determine the depth of the sensor in detecting color and the system's efficiency in the sorting process. The experimental results show that the system can perform classification with high accuracy and improve sorting efficiency compared to manual methods. This technology is designed to make the chili sorting process faster and more accurate and can be applied on an industrial scale to increase the productivity and quality of agricultural products.*

Keywords *– Chili Classification; TCS3200; Internet of Things; Automatic sorting; Smart Farming.*

1. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi mendorong penggunaan sistem otomatis yang lebih efisien dalam berbagai bidang, termasuk pertanian [1]. Mikrokontroler seperti ESP32 dan sensor warna TCS3200 memungkinkan pengembangan 2sistem cerdas untuk mengklasifikasikan objek secara akurat dan *real-time* [2]. Di sisi lain, meningkatnya permintaan pasar terhadap cabai berkualitas unggul menuntut proses pemilahan yang cepat dan konsisten, sementara metode manual yang masih digunakan petani dinilai kurang efisien, memakan waktu, dan berpotensi menghasilkan kualitas yang tidak seragam. Permasalahan tersebut juga terjadi di Desa Sindangheula, di mana proses sortasi cabai masih dilakukan secara manual dan menghadapi berbagai kendala, seperti ketidakkonsistenan hasil serta risiko kontaminasi dari cabai busuk. Oleh karena itu, diperlukan inovasi teknologi berupa sistem klasifikasi otomatis berbasis *Internet of Things* (IoT) dengan memanfaatkan sensor TCS3200 dan *Traction Control System* [3]. Sistem ini diharapkan mampu

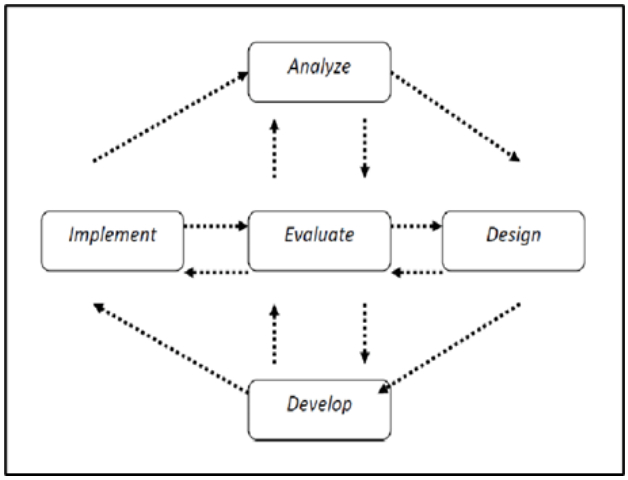
meningkatkan efisiensi, akurasi, serta kualitas hasil panen cabai, sehingga dapat mendukung peningkatan nilai ekonomi bagi petani.

2. METODE PENELITIAN

Metode penelitian yang diterapkan dalam studi ini menggunakan pendekatan *Research and Development* (*R&D*) dengan model pengembangan *ADDIE* (*Analyze*, *Design*, *Develop*, *Implement*, dan *Evaluate*) [4].

2.1. Analisa dan Arsitektur Sistem

Penelitian diawali dengan tahap analisis untuk mengidentifikasi masalah utama di Desa Sindangheula, yaitu proses pemilahan cabai yang masih manual, tidak konsisten, dan memakan waktu lama. Berdasarkan kebutuhan tersebut, dirancang sebuah arsitektur sistem otomatisasi berbasis *Internet of Things* (IoT) dengan mikrokontroler ESP32 sebagai unit kontrol pusat. Sistem ini mengintegrasikan sensor warna TCS3200 untuk mendeteksi nilai *RGB* dari buah cabai guna menentukan tingkat kematangannya (hijau atau merah) [5]. Selain itu, arsitektur perangkat keras mencakup penggunaan Motor *Gearbox DC* yang dikendalikan melalui sistem kontrol traksi (*Traction Control System*/*TCS*) untuk menjaga stabilitas kecepatan konveyor serta meminimalkan slip.



Gambar. 1 Metode Penelitian R&D

2.2. Metode Penyelesaian Masalah

Untuk menyelesaikan masalah akurasi dan efisiensi, penulis menerapkan algoritma logika *IF-ELSE* dalam pengolahan data. Frekuensi warna yang ditangkap oleh sensor TCS3200 dikonversi menjadi parameter *RGB*, yang kemudian diklasifikasikan ke dalam kategori warna tertentu melalui program yang ditanamkan pada ESP32 [6]. Guna mengatasi keterbatasan pemantauan jarak jauh, sistem ini diintegrasikan dengan *Telegram Bot*. Hal ini memungkinkan pengiriman notifikasi dan laporan hasil klasifikasi secara *real-time* kepada petani melalui jaringan internet, sehingga efektivitas operasional dapat dipantau dari mana saja.

2.3. Implementasi Sistem

Implementasi dilakukan dengan merakit perangkat keras dan perangkat lunak secara terintegrasi. Perangkat keras mencakup pemasangan sensor warna di dalam ruang pemindaian tertutup (kotak gelap) untuk menjaga konsistensi pembacaan *RGB* dari gangguan cahaya luar. Sementara itu, perangkat lunak dibangun menggunakan *Arduino IDE* dengan bahasa pemrograman C++. Implementasi IoT mencakup konfigurasi

protokol keamanan *SSL* melalui *library WiFiClientSecure* untuk memastikan koneksi yang aman antara ESP32 dan *server* Telegram [7].

2.4 Pengujian dan Hasil

Tahap akhir adalah evaluasi melalui pengujian sistem secara menyeluruh untuk memvalidasi akurasi pembacaan sensor dan stabilitas mekanisme mekanis. Hasil pengujian menunjukkan bahwa integrasi IoT melalui *Telegram Bot* berjalan lancar tanpa gangguan, memungkinkan pemantauan jumlah klasifikasi cabai dan status operasional mesin secara efisien dan akurat. Dengan demikian, metode ini terbukti mampu meningkatkan kecepatan serta akurasi proses penyortiran dibandingkan dengan metode manual.

3. HASIL DAN PEMBAHASAN

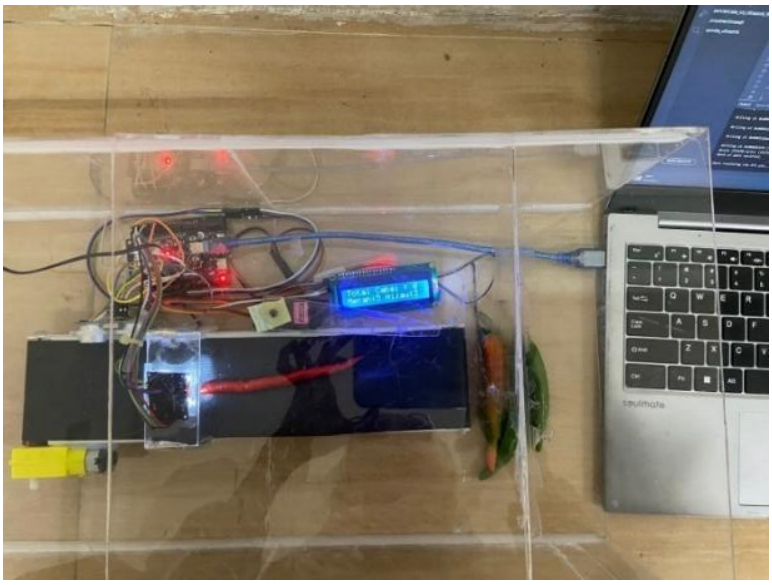
3.1 Hasil

Perancangan perangkat keras sistem ini menggunakan komponen spesifik untuk mendukung kinerja yang stabil dan efisien. Motor *Gearbox DC* digunakan untuk menghasilkan putaran yang stabil pada kecepatan rendah, sementara relay berfungsi sebagai pengendali aliran listrik ke motor. Penambahan resistor 10 Ohm bertujuan membatasi lonjakan arus awal (*inrush current*), sehingga pergerakan konveyor menjadi lebih halus, menjaga kestabilan cabai, dan mengurangi risiko kerusakan. Pengolahan data dikendalikan oleh mikrokontroler ESP32 yang terintegrasi dengan sistem IoT. Sensor TCS3200 ditempatkan dalam ruang tertutup dengan pencahayaan konstan agar pembacaan warna *RGB* lebih akurat dan konsisten. Meskipun *relay* bekerja secara *on/off*, algoritma *Traction Control System* (*TCS*) pada ESP32 mengatur durasi kerja motor secara presisi untuk menjaga sinkronisasi dengan proses pemindaian. Hasil klasifikasi kemudian diteruskan ke sistem penyortir dan dikirim ke *platform cloud* untuk pemantauan secara *real-time*.

3.1.1 Gambar Hasil Uji Coba

Perancangan *Hardware* dengan mikrokontroler ESP32 berfungsi sebagai pusat kontrol utama. Untuk menjalankan ESP32 dan semua modul pendukung, termasuk sensor warna TCS3200, modul *Relay* 1 *Channel*, dan *Motor DC Gearbox*, sistem ini menggunakan satu daya DC yang stabil. Agar pergerakan mekanik konveyor tetap lancar tanpa slip, yang dapat merusak kualitas fisik cabai, resistor 10 Ohm digunakan dalam rangkaian daya untuk berfungsi sebagai pengatur arus awal.

Gambar 1. Hasil Perakitan Alat



Gambar 2. Hasil Uji Coba Alat

Hasil uji coba pada bot Telegram menunjukkan bahwa sistem mampu mengirimkan notifikasi statistik jumlah cabai merah dan hijau secara *real-time* segera setelah sensor warna melakukan klasifikasi di jalur konveyor.

Gambar 3. Hasil Uji Coba Di Telegram Boot

3.1.2 Hasil Pengujian Sistem

Tabel 1. Hasil Pengujian

No	Komponen	Pengujian	Hasil yang Diharapkan	Logika (Ya/Tidak)
1	Sensor Ultrasonik	Cabai berada pada jarak deteksi yang ditentukan.	Sistem mendeteksi adanya objek dan memicu proses pemindaian warna.	Ya
2	Sensor Warna (Klasifikasi)	Cabai berwarna merah diletakkan di bawah sensor.	Sistem mengklasifikasikan objek sebagai Cabai Matang.	Ya
3	Sensor Warna (Klasifikasi)	Cabai berwarna hijau diletakkan di bawah sensor.	Sistem mengklasifikasikan objek sebagai Cabai Mentah.	Ya
4	Sensor Warna (Klasifikasi)	Cabai berwarna kuning diletakkan di bawah sensor.	Sistem mengklasifikasikan objek sebagai Cabai Kuning.	Tidak
5	Mekanik Pemilah	Perintah pemisahan dikirim setelah klasifikasi warna.	*Servo* memindahkan cabai ke wadah yang benar.	ya
6	Konektivitas IoT	Data hasil pemilahan dikirim ke Aplikasi Telegram Bot	Dashboard IoT menampilkan jumlah dan status klasifikasi secara *real-time*.	ya

3.2 Pembahasan

Perancangan perangkat keras sistem ini menggunakan komponen spesifik untuk mendukung kinerja yang stabil dan efisien. Motor *Gearbox DC* digunakan untuk menghasilkan putaran yang stabil pada kecepatan rendah, sementara *relay* berfungsi sebagai pengendali aliran listrik ke motor. Penambahan *resistor* 10 Ohm bertujuan membatasi lonjakan arus awal (*inrush current*), sehingga pergerakan konveyor menjadi lebih halus, menjaga kestabilan cabai, dan mengurangi risiko kerusakan []. Pengolahan data dikendalikan oleh mikrokontroler ESP32 yang terintegrasi dengan sistem IoT. Sensor TCS3200 ditempatkan dalam ruang tertutup dengan pencahayaan konstan agar pembacaan warna *RGB* lebih akurat dan konsisten. Meskipun *relay* bekerja secara *on/off*, algoritma *Traction Control System* (*TCS*) pada ESP32 mengatur durasi kerja motor secara presisi untuk menjaga sinkronisasi dengan proses pemindaian. Hasil klasifikasi kemudian diteruskan ke sistem penyortir dan dikirim ke *platform cloud* untuk pemantauan secara *real-time*.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa prototipe sistem klasifikasi buah cabai otomatis ini telah berhasil dirancang dan diimplementasikan dengan tingkat akurasi mencapai 92% dalam membedakan warna merah dan hijau. Keberhasilan mekanis sistem didukung oleh penerapan *Traction Control System* (TCS) sederhana yang menggunakan resistor untuk menstabilkan arus motor, sehingga konveyor bergerak lebih halus dan mampu meminimalisir guncangan atau slip pada buah saat proses pemindaian berlangsung. Selain itu, integrasi mikrokontroler ESP32 dengan platform *Internet of Things* (IoT) memungkinkan pengiriman data statistik hasil panen secara *real-time* kepada petani melalui aplikasi Telegram, yang secara signifikan mengurangi ketergantungan pada proses penyortiran manual yang bersifat subjektif. Secara keseluruhan, alat ini terbukti efektif menjadi solusi teknologi tepat guna dalam menjaga standarisasi kualitas pascapanen bagi petani di Desa Sindangheula.

DAFTAR PUSTAKA

[1] S. Achmady, L. Qadriah, and A. Auzan, "Rancang Bangun Magnetic Solenoid Door Lock Dengan Speech Recognition Menggunakan Nodemcu Berbasis Android," Jurnal Real Riset, vol. 4, no. 2, pp. 79–91, 2022.

[2] S. T. Ade Sumaedi, M. K. Angelina Hadriani, and S.kom., Teknologi Otomatisasi Sistem Kontrol Base On Mikrokontroler, M. K. T. H. H. Samosir, Ed. Indonesia: GEMILANG PRESS INDONESIA, 2025.

[3] S. Adrean and S. Yulia Putri, "SISTEM KUNCI OTOMATIS BERBASIS ARDUINO UNO DI PT JAYASEGAR BERKAT MANDIRI 1Syachri," Paper Knowledge. Toward a Media History of Documents, vol. 2, no. 1, pp. 12–26, 2022.

[4] R. S. Akbar et al., "Prototype Mesin Conveyor Pemilah Otomatis Berbasis IoT (Internet of Things) Universitas Dian Nusantara, Jakarta, Indonesia," Sep. 2025.

[5] F. D. Azzahra, R. Hidayati, and K. Sari, "MENGGUNAKAN METODE K-NEAREST NEIGHBOR," n.d.

[6] U. Hanik, "DETEKSI TINGKAT KEMATANGAN CABAI RAWIT (CAPSICUM FRUTESCENS) MENGGUNAKAN SENSOR WARNA TCS3200 BERBASIS ARDUINO UNO," Braz Dent J., vol. 33, no. 1, 2022.

[7] G. B. Hendratri, J. Iswanto, A. Tohawi, and A. Yuli Dianto, "Pengaruh Fluktuasi Harga Cabai Rawit dan Dampaknya pada Daya Beli Konsumen di Pasar Wage Nganjuk," Kolaboratif Sains, vol. 6, no. 11, pp. 1595–1600, 2023.

[8] Ilyas, "Pengenalan tanaman cabai dengan teknik klasifikasi menggunakan metode cnn," Senamika, pp. 15–22, 2020.

[9] J. Burdadi, R. Ridwan, and I. Nugraha, "APLIKASI SENSOR WARNA TCS3200 PADA SISTEM PENYORTIRAN BARANG BERBASIS INTERNET OF THINGS (IOT)," in Prosiding Seminar Nasional Inovasi Teknologi Terapan, 2022, pp. 141–145.

[10] P. M. Kumar and A. Deepak, "Comparison of Piezo Resistive Property of Graphene based Polymer Films and Carbon Nanotube based Polymer Films to Optimize the Conductivity," Geintec, vol. 11, no. 2, pp. 1324–1338, 2021.

[11] A. R. Kurniadi, A. P. Supriyadi, A. P. Pambudi, M. R. Fazryansah, and R. Hidayat, "BUAH TOMAT BERDASARKAN WARNA MENGGUNAKAN TCS3200 BERBASIS IOT," Jurnal Listrik Telekomunikasi Elektronika, vol. 22, no. 1, pp. 1–6, 2025.

[12] M. P. Lukman, A. S. Bakhtiar, and M. S. Pongsamma, "SISTEM PENYORTIR OTOMATIS KEMATANGAN TOMAT BERDASARKAN WARNA DENGAN SENSOR TCS3200 BERBASIS INTERNET OF THINGS," vol. 01, no. 01, pp. 1–7, 2023.

[13] S. M. Zaki, "Kajian tentang Perumusan Hipotesis Statistik Dalam Pengujian Hipotesis Penelitian," Jurnal Ilmiah Ilmu Pendidikan, vol. 4, pp. 115–118, 2021.

[14] D. N. Masmur and M. Snae, "Rancang bangun sistem sortir buah cabai berdasarkan warna berbasis arduino uno," Jurnal Teknologi Informasi, vol. 15, no. c, pp. 33–42, 2024.

Jicom : Journal Information & Computer
Volume 4, Nomor 2, Juli 2024, hlm. 74-82
DOI : 10.32493/jicomisc.v2i1.37666
.

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Perancangan Sistem Informasi Laporan Kegiatan Bidang Konservasi Dan Pertamanan Berbasis Android Dengan Metode Scrum

Muhammad Rangga Junior G*[1], Ari Mulyoto [2]
[1,2)]ProgramStudi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pamulang
Email: [*1] *junior.gautama@gmail.com*

(Naskah masuk: *8 Juni 2026*, diterima untuk diterbitkan: *31 Juli 2026*)

Abstrak: *Perkembangan teknologi informasi mendorong instansi pemerintah untuk meningkatkan efektivitas dan efisiensi dalam pengelolaan data serta pelaporan kegiatan. Salah satu permasalahan yang sering dihadapi pada bidang konservasi sumber daya alam dan pertamanan adalah proses pelaporan kegiatan yang masih dilakukan secara manual, sehingga berpotensi menimbulkan keterlambatan, ketidakteraturan data, serta kesulitan dalam monitoring kegiatan. Penelitian ini bertujuan untuk merancang dan membangun sistem laporan kegiatan bidang konservasi sumber daya alam dan pertamanan berbasis Android dengan menggunakan metode Scrum. Metode Scrum dipilih karena mampu mendukung pengembangan sistem secara iteratif, fleksibel, dan berorientasi pada kebutuhan pengguna. Sistem yang dirancang memiliki fitur pengelolaan laporan kegiatan, dokumentasi berupa foto dan data pendukung, manajemen pengguna berdasarkan hak akses, serta pencatatan aktivitas pengguna. Perancangan sistem meliputi pembuatan Entity Relationship Diagram (ERD), Logical Record Structure (LRS), dan normalisasi basis data untuk memastikan integritas dan keandalan data. Hasil dari penelitian ini diharapkan dapat menghasilkan sistem pelaporan yang terintegrasi, mudah digunakan, serta mampu meningkatkan efektivitas, transparansi, dan akuntabilitas dalam pengelolaan kegiatan konservasi dan pertamanan.*

Kata Kunci *– Android, Sistem Informasi, Konservasi, Pertamanan, Scrum.*

Abstract: *The development of information technology encourages government institutions to improve effectiveness and efficiency in data management and activity reporting. One of the problems frequently encountered in the field of natural resource conservation and landscaping is that activity reporting is still carried out manually, which can lead to delays, data inconsistency, and difficulties in monitoring activities. This study aims to design and develop an Android-based activity reporting system for the field of natural resource conservation and landscaping using the Scrum method. The Scrum method was selected because it supports iterative, flexible, and user-oriented system development. The proposed system provides features for activity report management, documentation in the form of photos and supporting data, user management based on access rights, and user activity logging. The system design includes the development of an Entity Relationship Diagram (ERD), Logical Record Structure (LRS), and database normalization to ensure data integrity and reliability. The results of this study are expected to produce an integrated and user-friendly reporting system that can enhance effectiveness, transparency, and accountability in managing conservation and landscaping activities.*

Keywords – *Android, Information System, Conservation, Landscaping, Scrum.*

1. PENDAHULUAN

Dinas Lingkungan Hidup dan Kebersihan Kabupaten Tangerang memiliki peran penting dalam menjaga kelestarian sumber daya alam (SDA) dan pengelolaan pertamanan di wilayahnya. Dalam hal pencapaian suatu tujuan yang akan dicapai di perlukan suatu perencanaan dan tindakan nyata untuk dapat mewujudkannya, secara umum bisa di katakan bahwa Visi dan Misi adalah suatu konsep perencanaan yang di sertai dengan tindakan sesuai dengan apa yang di rencanakan untuk mencapai suatu tujuan [1]. Namun, dalam menjalankan tugas tersebut, dinas menghadapi berbagai tantangan, terutama dalam pengumpulan, pemantauan, dan pelaporan data kegiatan konservasi SDA dan pertamanan. Proses pelaporan yang masih dilakukan secara manual dan terpisah kerap menimbulkan keterlambatan penyampaian informasi, kurangnya akurasi data, serta kesulitan dalam melakukan analisis data secara menyeluruh [2]. Kondisi ini berdampak langsung pada kualitas pengambilan keputusan, yang pada akhirnya memengaruhi efektivitas program konservasi yang dirancang dan dilaksanakan [3]. Proses manual yang digunakan tidak hanya memakan waktu, tetapi juga menyulitkan petugas

lapangan dalam menyampaikan laporan secara cepat dan sistematis. Akibatnya, data yang diterima sering kali tidak sinkron dengan kondisi nyata di lapangan, sehingga memengaruhi kecepatan dinas dalam merespons kebutuhan atau permasalahan yang muncul. Selain itu, minimnya transparansi dan sistem monitoring secara real-time menjadi kendala utama dalam memastikan seluruh kegiatan terlaksana sesuai dengan perencanaan dan target yang telah ditetapkan, sehingga efisiensi dan akuntabilitas kinerja dinas belum dapat tercapai secara optimal [4].

Melihat permasalahan tersebut, diperlukan solusi teknologi yang dapat mengatasi tantangan ini secara komprehensif. Salah satu solusi yang diusulkan adalah pengembangan aplikasi berbasis Android yang dirancang khusus untuk mendukung proses pelaporan kegiatan konservasi SDA dan pertamanan secara real-time. Dalam proses pengembangannya, diterapkan metode *Scrum* sebagai pendekatan *agile* yang bersifat iteratif dan melibatkan pengguna secara aktif di setiap tahap pengembangan, sehingga aplikasi yang dihasilkan lebih responsif terhadap kebutuhan dan tantangan di lapangan [5]. Dengan pendekatan ini, proses pelaporan yang sebelumnya manual dapat diotomatisasi, mengurangi risiko kesalahan, mempercepat distribusi informasi, dan meningkatkan efisiensi secara keseluruhan [6].

Keberadaan aplikasi ini diharapkan dapat meningkatkan kinerja operasional Dinas Lingkungan Hidup dan Kebersihan Kabupaten Tangerang secara signifikan. Aplikasi ini tidak hanya berfungsi sebagai alat bantu teknis, tetapi juga sebagai langkah strategis dalam mendukung upaya pelestarian lingkungan, pencapaian tujuan pembangunan berkelanjutan, dan peningkatan kualitas hidup masyarakat di Kabupaten Tangerang. Dengan data yang lebih terorganisir dan aksesibilitas yang lebih tinggi, dinas dapat melakukan perencanaan, monitoring, dan evaluasi program secara lebih efektif.

2. METODE PENELITIAN

Metode Penelitian (bisa meliputi analisa, arsitektur, metode yang dipakai untuk menyelesaikan masalah, implementasi), dalam bahasan ini penulis bisa menguraikan bagaimana penelitian tersebut dilakukan.

Penelitian ini menggunakan pendekatan kualitatif yang berfokus pada perancangan dan pengembangan sistem informasi berbasis Android. Pendekatan ini dipilih karena relevan dalam menggambarkan kondisi nyata di lapangan serta menghasilkan solusi teknologi yang sesuai dengan kebutuhan instansi. Metode pengembangan sistem yang diterapkan adalah Scrum, yakni salah satu kerangka kerja *agile* yang memungkinkan proses pengembangan perangkat lunak berlangsung secara iteratif, adaptif, dan terstruktur [7]. Penerapan metode ini dianggap sesuai mengingat kompleksitas kebutuhan sistem yang dapat berkembang seiring berjalannya proses pengembangan di lapangan.

Pengumpulan data dalam penelitian ini dilaksanakan melalui tiga instrumen utama. Studi literatur digunakan untuk memperoleh landasan teori yang kuat melalui kajian terhadap jurnal ilmiah, buku referensi, serta skripsi yang relevan dengan topik penelitian. Wawancara terstruktur dilakukan kepada pihak Dinas Lingkungan Hidup dan Kebersihan Kabupaten Tangerang guna memperoleh data primer berupa gambaran kebutuhan fungsional sistem yang akan dikembangkan. Observasi lapangan dilaksanakan secara sistematis untuk memperoleh pemahaman mendalam terhadap kondisi aktual proses pelaporan yang berjalan, sehingga permasalahan yang ada dapat teridentifikasi secara komprehensif.

Pengembangan sistem dalam penelitian ini mengacu pada kerangka kerja Scrum yang terdiri atas serangkaian siklus pengembangan terstruktur. Proses diawali dengan penyusunan *Product Backlog* sebagai dokumentasi seluruh kebutuhan dan prioritas fitur sistem. Selanjutnya, *Sprint Planning* dilakukan untuk menentukan ruang lingkup pekerjaan dalam setiap periode sprint. Selama *Sprint Execution* berlangsung, aktivitas pengembangan dipantau melalui *daily stand-up meeting* guna mengidentifikasi hambatan secara dini. Setiap akhir sprint, *Sprint Review* dan *Sprint Retrospective* dilaksanakan masing-masing untuk memperoleh umpan balik dari *stakeholder* dan mengevaluasi efektivitas proses kerja tim. Hasil dari setiap siklus sprint berupa *increment* yang dapat dioperasikan, dan perbaikan berkelanjutan (*Continuous Improvement*) dilakukan secara konsisten berdasarkan masukan yang diperoleh pada setiap siklus [8].

Implementasi sistem dilaksanakan menggunakan *android studio* sebagai *Integrated Development Environment* (IDE) utama dalam pembangunan aplikasi berbasis Android. Lingkup implementasi mencakup perancangan antarmuka pengguna (*User Interface*), pengintegrasian modul input data kegiatan, serta pengembangan fitur dokumentasi visual berupa unggahan foto bukti kegiatan. Validasi sistem dilakukan melalui dua metode pengujian, yaitu *Functional Testing* untuk memverifikasi bahwa seluruh fitur aplikasi berjalan sesuai dengan spesifikasi kebutuhan pengguna, serta *Compatibility Testing* untuk memastikan aplikasi dapat beroperasi secara optimal pada berbagai perangkat Android dengan beragam versi sistem operasi,

sehingga aplikasi memiliki jangkauan penggunaan yang luas di lingkungan Dinas Lingkungan Hidup dan Kebersihan Kabupaten Tangerang.

3. HASIL DAN PEMBAHASAN

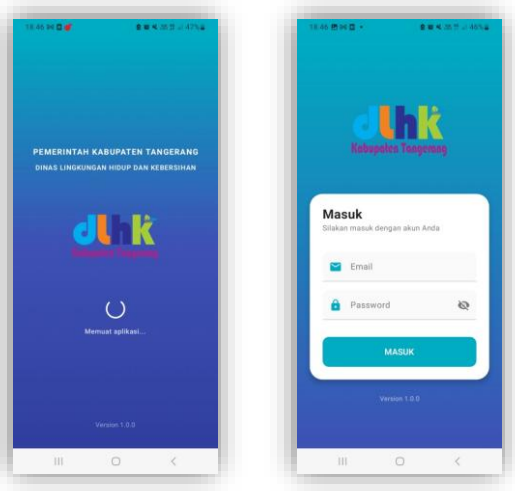
3.1. Hasil

Bagian Hasil memuat pemaparan temuan penelitian serta analisis yang diperoleh berdasarkan pengujian yang telah dilakukan. Penyajian hasil dapat dilakukan secara deskriptif, baik secara kualitatif maupun kuantitatif, sesuai dengan karakteristik data yang digunakan.

A. Implementasi Fitur

1. Implementasi *Login*

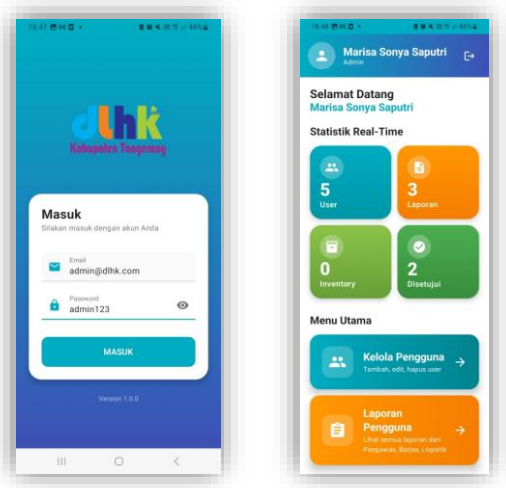
merupakan tahap awal yang harus dilakukan oleh *Admin* dan pengguna untuk mengakses aplikasi laporan kegiatan konservasi. Pada halaman ini, pengguna diminta memasukkan email dan *Password* yang telah terdaftar sebagai proses autentikasi.



Gambar 1. Implementasi Login

2. Implementasi *Login Dashboard Admin*

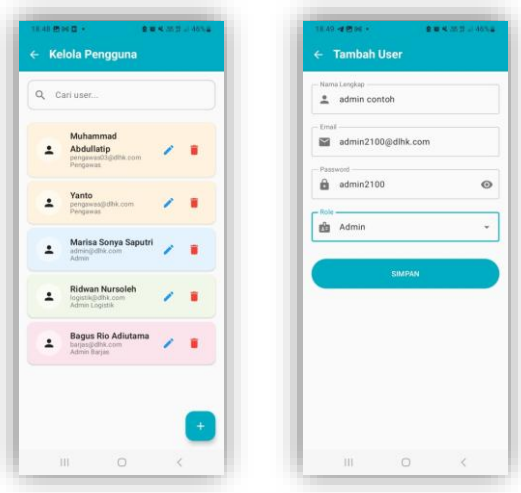
Berfungsi sebagai tahap awal bagi *Admin* untuk mengakses dan mengelola seluruh fitur aplikasi. *Admin* diwajibkan memasukkan email dan *Password* yang telah terdaftar untuk memastikan bahwa hanya pengguna dengan hak akses *Admin* yang dapat masuk ke dalam sistem. Setelah proses autentikasi berhasil, sistem akan menampilkan halaman *Dashboard Admin* yang berisi berbagai menu pengelolaan, seperti manajemen pengguna, laporan kegiata. Apabila data *Login* tidak sesuai.



Gambar 2. Implementasi *Dashboard Admin*

3. Implementasi *Admin* Kelola Pengguna

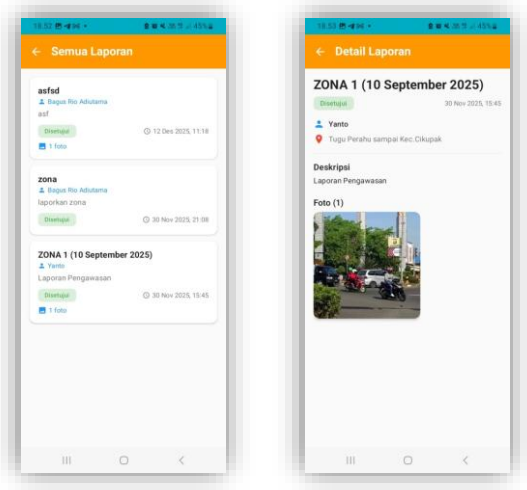
Digunakan untuk menampilkan dan mengelola data pengguna yang terdaftar dalam aplikasi. Pada halaman ini, *Admin* dapat melihat daftar pengguna yang telah ditambahkan, termasuk informasi dasar pengguna sesuai dengan data yang tersimpan di dalam sistem. Melalui halaman kelola pengguna, *Admin* memiliki akses untuk melakukan penambahan pengguna baru, mengubah data pengguna, serta menghapus pengguna yang sudah tidak aktif. Fitur ini bertujuan untuk memastikan pengelolaan hak akses dan data pengguna tetap terkontrol dengan baik.



Gambar 3. Implementasi *Admin* Kelola Pengguna

4. Implementasi *Admin* Laporan Pengguna

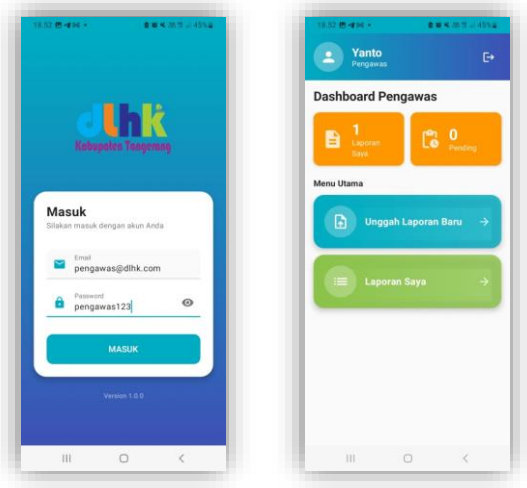
Digunakan untuk menampilkan seluruh laporan kegiatan yang dikirimkan oleh pengguna melalui aplikasi. *Admin* dapat melihat daftar laporan pengguna yang tersimpan di dalam sistem. Selain melihat daftar laporan, *Admin* juga dapat mengakses detail laporan pengguna untuk mengetahui informasi lebih lengkap, seperti deskripsi kegiatan, waktu pelaksanaan, serta dokumentasi pendukung. Fitur ini bertujuan untuk membantu *Admin* dalam melakukan pengawasan laporan kegiatan terstruktur.



Gambar 4. Implementasi *Admin* Laporan Pengguna

5. Implementasi *Login Dashboard* Pengawas

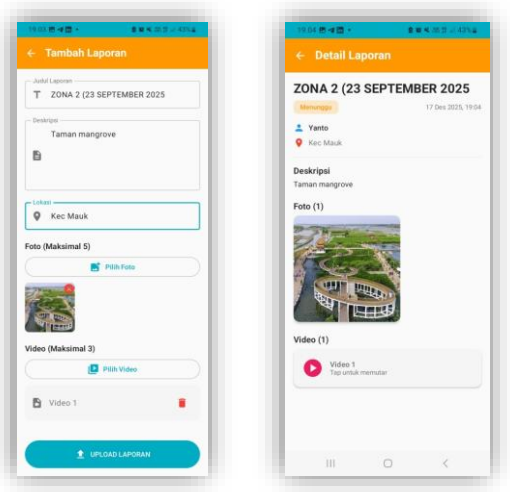
Berfungsi sebagai tahap awal bagi *Admin* untuk mengakses dan mengelola seluruh fitur aplikasi. Pengawas diwajibkan memasukkan email dan *Password* yang telah terdaftar untuk memastikan bahwa hanya pengguna dengan hak akses *Admin* yang dapat masuk ke dalam sistem. Setelah proses autentikasi berhasil, sistem akan menampilkan halaman *Dashboard* Pengawas yang berisi berbagai menu pengelolaan, seperti manajemen Pengawas, Unggah laporan, Laporan Pengawas. Apabila data *Login* tidak sesuai,



Gambar 5. Implementasi *Login Dashboard* Pengawas

6. Implementasi Pengawas Tambah Laporan

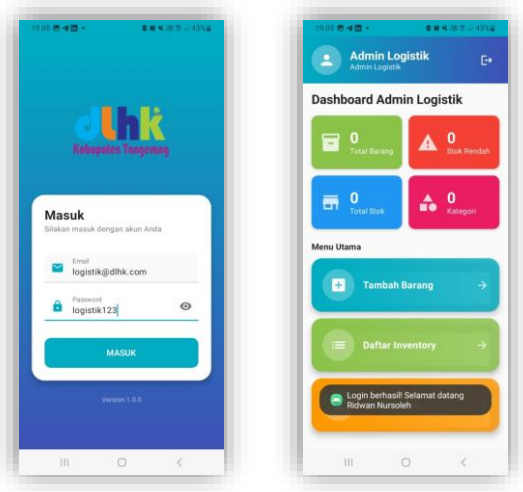
Digunakan oleh pengawas memasukkan data laporan kegiatan ke dalam sistem aplikasi, pengawas dapat mengisi *form* laporan yang terdiri dari judul laporan, deskripsi kegiatan, lokasi pelaksanaan, menambahkan dokumentasi pendukung berupa foto dan video, Setelah seluruh data laporan diisi dengan lengkap, pengawas dapat mengunggah laporan melalui tombol upload laporan. Data yang dikirimkan akan tersimpan di dalam sistem dan diteruskan kepada *Admin* untuk dilakukan proses peninjauan dan persetujuan.



Gambar 6. Implementasi Pengawas Tambah Laporan

7. Implementasi *Login Admin* Logistik *Dashboard*

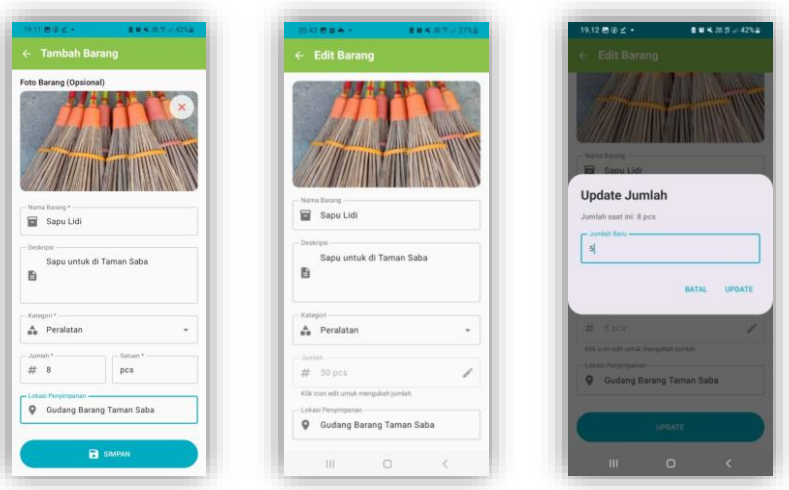
Berfungsi sebagai tahap awal bagi *Admin* untuk mengakses dan mengelola seluruh fitur aplikasi. Pengawas diwajibkan memasukkan email dan *Password* yang telah terdaftar untuk memastikan bahwa hanya pengguna dengan hak akses *Admin* yang dapat masuk ke dalam sistem. Setelah proses autentikasi berhasil, sistem akan menampilkan halaman *Dashboard Admin* Logistik yang berisi berbagai menu pengelolaan, seperti manajemen Inventory Barang, Tambah Barang, Daftar Inventory.



Gambar 7. Implementasi *Login Admin* Logistik *Dashboard*

8. Implementasi *Admin* Logistik Tambah Barang dan Update Jumlah Barang

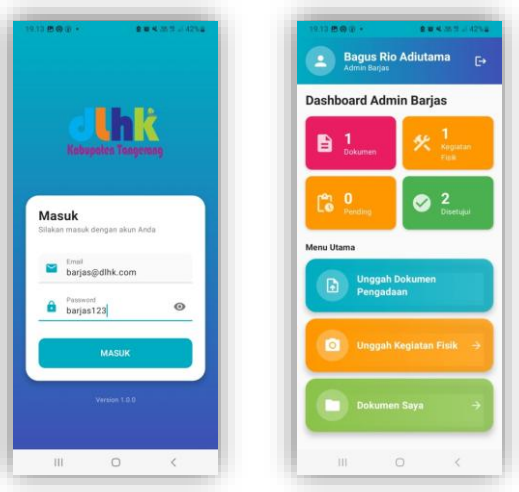
Digunakan untuk menambahkan data barang logistik ke dalam sistem aplikasi. *Admin* logistik dapat mengisi form yang tersedia, meliputi nama barang, deskripsi, kategori barang, jumlah, satuan, serta lokasi penyimpanan. *Admin* juga dapat menambahkan foto barang sebagai dokumentasi pendukung. Setelah seluruh data diisi dengan lengkap, *Admin* logistik dapat menyimpan data barang ke dalam sistem melalui tombol simpan. Data yang tersimpan akan digunakan untuk keperluan pengelolaan inventaris logistik secara terstruktur dan akurat.



Gambar 8. Implementasi *Login Admin* Logistik *Dashboard*

9. Implementasi *Login Admin* barjas *Dashboard*

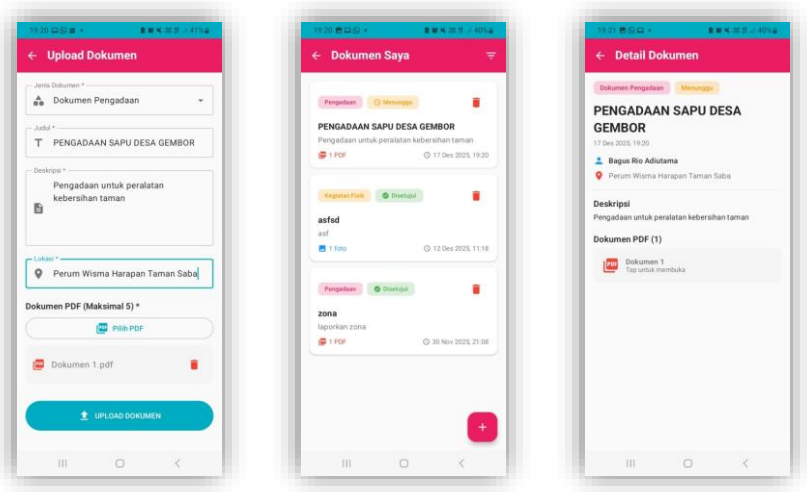
berfungsi sebagai tahap awal bagi *Admin* untuk mengakses dan mengelola seluruh fitur aplikasi. Pengawas diwajibkan memasukkan email dan *Password* yang telah terdaftar untuk memastikan bahwa hanya pengguna dengan hak akses *Admin* yang dapat masuk ke dalam sistem. Setelah proses autentikasi berhasil, sistem akan menampilkan halaman *Dashboard Admin* Barjas yang berisi berbagai menu Unggah Dokumen Pengadaan, Unggah Dokumen Pengadaan, Dokumen Laporan yang sudah dibuat,



Gambar 9. Implementasi *Login Admin* barjas *Dashboard*

10. Implementasi *Admin* Barjas *Upload* Dokumen

Digunakan untuk mengunggah dokumen pendukung ke dalam sistem aplikasi. Pada halaman ini, *Admin* mengisi form yang terdiri dari jenis dokumen, judul dokumen, deskripsi, dan lokasi, serta memilih file dokumen dalam format *PDF* sebagai berkas yang akan diunggah, Setelah seluruh data diisi dengan lengkap, *Admin* dapat mengunggah dokumen ke dalam sistem melalui fitur upload. Dokumen yang berhasil diunggah akan tersimpan di basis data dan dapat diakses sesuai dengan kebutuhan pengguna aplikasi, Fitur ini bertujuan untuk mempermudah pengelolaan dan penyimpanan dokumen secara terstruktur dan aman.



Gambar 10. Implementasi *Login Admin* barjas *Dashboard*

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa perancangan sistem informasi laporan kegiatan bidang konservasi dan pertamanan berbasis Android dengan metode Scrum mampu memberikan solusi terhadap permasalahan proses pelaporan kegiatan yang sebelumnya masih dilakukan secara manual. Sistem yang dikembangkan dapat membantu proses pengelolaan laporan kegiatan menjadi lebih efektif, terstruktur, dan mudah diakses oleh setiap pengguna sesuai dengan hak akses yang dimiliki.

Selain itu, implementasi fitur dokumentasi digital berupa unggahan foto, video, dan dokumen pendukung memberikan kemudahan dalam proses pengarsipan data kegiatan dan pengelolaan inventaris logistik. Dengan adanya sistem ini, transparansi, akuntabilitas, dan efisiensi kerja dalam pelaksanaan kegiatan konservasi dan pertamanan dapat meningkat secara lebih optimal dibandingkan dengan sistem manual sebelumnya.

Meskipun demikian, penelitian ini masih memiliki beberapa keterbatasan, terutama pada ketergantungan aplikasi terhadap koneksi internet saat proses pengiriman data berlangsung. Oleh karena itu, pengembangan lanjutan disarankan untuk menambahkan fitur mode *offline* agar aplikasi tetap dapat digunakan ketika jaringan internet tidak tersedia atau tidak stabil. Selain itu, diperlukan pengembangan pada aspek keamanan data, integrasi notifikasi otomatis, serta peningkatan tampilan antarmuka pengguna agar sistem menjadi lebih optimal dan mudah digunakan oleh seluruh pengguna.

Penelitian selanjutnya juga diharapkan dapat mengembangkan sistem dengan cakupan yang lebih luas, seperti integrasi dengan sistem informasi lingkungan hidup lainnya atau penerapan teknologi berbasis *Geographic Information System* (GIS) untuk mendukung pemetaan lokasi kegiatan konservasi dan pertamanan secara lebih akurat dan informatif.

DAFTAR PUSTAKA

[1] Iriawan, M. R., & Ardhiansyah, M. (2023). PERANCANGAN APLIKASI MONITORING SATPAM BERBASIS ANDROID MENGGUNAKAN METODE SCRUM (PT. PARADUTA SERVICE INDONESIA). *Jurnal Penelitian Ilmu Komputer*, 69-81.

[2] Kebersihan, A. L. (2023, Oktober 25). *Visi dan Misi*. Retrieved from dlhk tangerangkab : https://dlhk.tangerangkab.go.id/profil-konten/42

[3] Laitupa, S. (2021). PENGATURAN KAWASAN KONSERVASI SUMBER DAYA ALAM HAYATI LAUT. *Jurnal Hukum Unsulbar*, 1-21.

[4] Patappari, A., Syafei, A. M., & Nurnaningsih. (2021). PERANCANGAN APLIKASI PENYEWAAN RUANG MEETING BEBASIS WEB PADA HOTEL GRAND AISHA SOPPENG. *Jurnal Ilmiah Sistem Informasi dan Teknik Informatika "JISTI"*, 39-49.

[5] Putra, D. J., & Tanaem, P. F. (2022). Perancangan Aplikasi Pembukuan Menggunakan Metode Agile Scrum. *Jurnal Teknik Informatika dan Sistem Informasi*, 509-521.

[6] Setyawan, R. A. (2024). Penerapan Firebase Realtime Database Pada Aplikasi Catatan Harian Diabetes Melitus. *Jurnal Informatika Komputer, Bisnis Dan Manajemen*, 1-9.

[7] Sibuea, S., Saputro, M. I., Annan, A., & Widodo, Y. B. (2022). Aplikasi Mobile Collection Berbasis Android Pada Pt. Suzuki Finance Indonesia. *Jurnal Informatika Dan Tekonologi Komputer (JITEK)*, 31–42.

[8] Wijaya, T. A., Menteng, C., Julianto, A., Surya, A., & Utami, E. (2021). Perancangan Desain Basis Data Sistem Informasi Geografis Tanah Penduduk Dengan Menerapkan Model Data Relasional (Studi Kasus : Desa Tumbang Mantuhe Kabupaten Gunung Mas Provinsi Kalimantan Tengah). *Jurnal Teknologi Informasi: Jurnal Keilmuan Dan Aplikasi Bidang Teknik Informatika*, 72–81.

Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 84-92
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Sistem Pemilah Limbah Organik dan Anorganik Berbasis IoT untuk Bank Sampah di Smp Terpadu Al-Qudwah

Burhanudin Raya Rambani[1], Agus Suhendi[2]
[1,2)]Program Studi Sistem Komputer, Universitas Pamulang Kampus Kota Serang
Email: [*1]brhnudeen1@gmail.com, [2]dosen10007@unpam.ac.id

(Naskah masuk: 30 Mei 2026, diterima untuk diterbitkan: 31 Juli 2026)

Abstrak: *Tempat sampah yang digunakan saat ini umumnya telah dipisahkan untuk sampah organik dan non-organik, namun dalam praktiknya masih banyak masyarakat yang keliru dalam menentukan jenis sampah sesuai kategorinya. Tujuan dari penelitian ini adalah perancangan smart bin, yakni tempat sampah pintar yang dirancang untuk memilah limbah organik dan anorganik secara otomatis. Komponen elektroniknya menggunakan mikrokontroller ESP32, sensor proximity kapasitif, induktif, ultrasonik, motor servo, dan lainnya. Sedangka bahannya memakai triplek, paku, dan kayu. Metode penelitian ini menggunakan kuantitatif dengan pendetakan eksperimental, dilakukan di SMP Terpadu Al-Qudwah, khusus kelas 9 Putri 1. Seluruh siswi merasa sangat puas dengan adanya tempat sampah pintar ini, akan tetapi secara uji black box, tempat sampah pintar ini dapat berfungsi namun beberapa kasus pemilahan kurang akurat. Seperti sampah daun yang seharusnya masuk ke organik, namun terkadang terdeteksi sebagai jenis anorganik.*

Kata Kunci *– smart bin, ESP32, sensor proximity*

Abstract: *Smart bin currently used are generally separated for organic and non-organic waste, but in practice, many people still make mistakes in determining the type of waste according to its category. The purpose of this study is to design a smart bin, namely a smart bin designed to sort organic and inorganic waste automatically. The electronic components use an ESP32 microcontroller, capacitive, inductive, and ultrasonic proximity sensors, servo motors, and more. The materials used are plywood, nails, and wood. This research method uses quantitative with experimental research, conducted at Al-Qudwah Integrated Junior High School, specifically for grade 9 Putri 1. All female students were very satisfied with the existence of this smart bin; however, in black box testing, this smart bin functions, but some cases of sorting are less accurate. Such as leaf litter that should be included in organic but is sometimes detected as inorganic.*

Keywords – *smart bin, ESP32, proximity sensor*

1. PENDAHULUAN

Sampah merupakan sesuatu yang tidak dipakai, tidak digunakan, tidak diinginkan, atau dibuang yang berasal dari aktivitas manusia dan tidak terjadi secara alami [1]. Berdasarkan sifatnya, sampah terbagi menjadi dua, yaitu organik dan anorganik. Sampah anorganik adalah jenis sampah yang tidak dapat terurai, seperti logam, kaca, dan plastik, sedangkan sampah organik mudah membusuk seperti sisa makanan, daun, dan buah-buahan [2].

Sampah organik merupakan limbah yang berasal dari sisa makhluk hidup, seperti hewan, manusia, dan tumbuhan, yang mengalami proses pembusukan atau pelapukan secara alami. Jenis sampah ini tergolong lebih ramah lingkungan karena dapat terurai oleh bakteri dan mikroorganisme lainnya dalam waktu yang relatif singkat tanpa menimbulkan dampak pencemaran jangka Panjang [3]. Limbah atau sampah anorganik merupakan jenis ampas yang sulit terurai secara alami (*non-biodegradable*), biasanya berupa bahan kering atau material sintetis yang tidak mudah membusuk dan memerlukan penanganan khusus dalam proses pengelolaannya [4].

Tempat sampah yang digunakan saat ini umumnya telah dipisahkan untuk sampah organik dan non-organik, namun dalam praktiknya masih banyak masyarakat yang keliru dalam menentukan jenis sampah sesuai kategorinya [5]. Pengelolaan yang baik, termasuk dalam hal pengolahan sampah dengan memisahkannya ke dalam kategori organik dan anorganik, bertujuan untuk mencegah timbulnya bau tidak sedap serta mengurangi risiko penyebaran penyakit [2].

Sistem pengelolaan sampah yang baik perlu diterapkan agar penanganan limbah lebih efektif dan berkelanjutan. Ketika sampah berhasil dipilah antara organik dan anorganik, maka limbah tersebut dapat dimanfaatkan kembali, terutama di lingkungan sekolah. Misalnya, sampah plastik dapat dijadikan bahan prakarya, sementara sisa makanan bisa diolah menjadi pupuk. Untuk mendukung proses ini, dibutuhkan teknologi yang mampu melakukan pemilahan sampah secara otomatis dan efisien. Salah satu teknologi yang dapat menjadi solusi adalah *smart bin*, yakni tempat sampah pintar yang dirancang untuk memilah sampah organik dan anorganik secara otomatis.

SMP Terpadu Al-Qudwah dipilih sebagai tempat penelitian, alasannya karena di sana sudah memiliki tempat sampah dengan dua jenis, yaitu organik dan anorganik, tetapi masih sering bercampur. Temuan tersebut menjadi acuan dalam pembuatan sistem pemilah sampah organik dan anorganik secara otomatis atau lebih dikenal dengan *smart bin.*

Dalam pembuatan *smart bin* diperlukan komponen yang mampu mendukung pengaplikasiannya, dan berikut di antaranya: ESP32 merupakan mikrokontroler yang kuat dan fleksibel, sangat sesuai untuk berbagai aplikasi *IoT* seperti sistem pemantauan dan pengendalian lingkungan. Perangkat ini sudah dilengkapi Wi-Fi dan Bluetooth terintegrasi, sehingga mendukung komunikasi nirkabel dan pemantauan dari jarak jauh [6].

Gambar 1. ESP32

Proximity kapasitif atau sensor kapasitif adalah perangkat yang dapat mendeteksi jarak dengan mengamati gerakan, komposisi kimia, tingkat dan komposisi cairan, serta tekanan. Sensor ini mampu mendeteksi bahan nonkonduktif seperti plastik atau kaca, dan bahan dielektrik seperti cairan. Oleh karena itu, sensor jenis ini berguna untuk mendeteksi kadar berbagai bahan melalui kaca, plastik, atau bahan instrumen lainnya [7].

Gambar 2. Sensor Proximity Kapasitif

Sensor proximity induktif adalah sensor yang mampu mendeteksi keberadaan objek tanpa kontak fisik, khususnya benda berbahan logam seperti besi, baja, atau aluminium. Selama objek berada dalam jarak deteksi (sensing distance), sensor akan merespons dengan mengubah nilai output-nya. Cara kerjanya adalah ketika tegangan diberikan, osilator akan menghasilkan medan magnet berfrekuensi tinggi pada kumparan induksi. Jika objek logam mendekati area sensing, medan magnet tersebut berubah. Perubahan ini kemudian ditangkap oleh rangkaian detektor (current sensor) dan diteruskan sebagai sinyal output sensor [8].

Gambar 3. Sensor Proximity Induktif

Sensor ultrasonik bekerja berdasarkan prinsip pantulan gelombang suara dan digunakan untuk mendeteksi keberadaan objek di depannya. Sensor ini beroperasi pada frekuensi di atas gelombang suara, yaitu antara 40 KHz hingga 400 KHz. Gelombang ultrasonik dihasilkan oleh rangkaian pemancar dan merambat dengan kecepatan sekitar 340 m/s. Ketika gelombang ini mengenai objek, gelombang akan dipantulkan kembali dan diterima oleh penerima ultrasonik. Sinyal yang diterima kemudian diproses untuk menghitung jarak antara sensor dan objek tersebut [9].

Gambar 4. Sensor Ultrasonik

Motor servo adalah motor DC yang telah dilengkapi dengan rangkaian pengendali internal sehingga dapat bergerak dengan presisi. Dalam penggunaannya, servo bekerja menggunakan sistem kontrol loop tertutup, memungkinkan posisi motor diatur dengan sangat tepat. Servo memiliki tiga kabel utama, yaitu Vcc, *ground*, dan sinyal data. Pengaplikasian PWM pada motor servo berbeda dengan PWM pada motor DC; pada servo, nilai PWM menentukan posisi tertentu yang harus dicapai, dan setelah posisi tersebut tercapai, motor akan berhenti [7].

Gambar 5. Motor Servo MG996R

LCD I2C adalah media tampilan yang mudah dibaca karena mampu menampilkan karakter dengan jelas dan memiliki area tampilan yang cukup luas. Modul ini dapat menampilkan hingga 32 karakter, masing-masing 16 karakter pada baris atas dan bawah. Secara standar, LCD membutuhkan 16 pin untuk proses kontrol, yang tentu tidak efisien. Oleh karena itu, digunakan modul driver I2C sehingga LCD dapat dikendalikan hanya dengan dua pin, yaitu SDA dan SCL, melalui jalur komunikasi I2C [10].

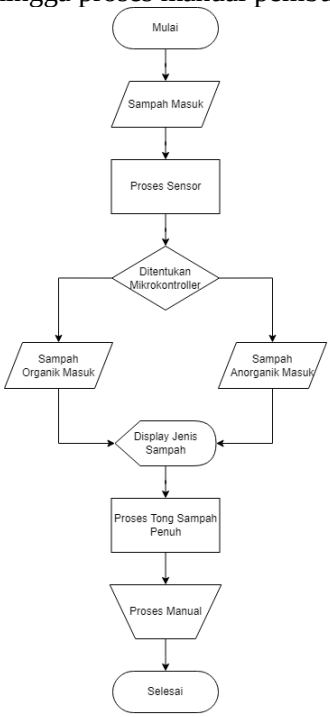
Gambar 6. LCD 12C

2. METODE PENELITIAN

Penelitian berjudul "Sistem Pemilah Limbah Organik dan Anorganik Berbasis *IoT* untuk Bank Sampah di SMP Terpadu Al-Qudwah" ini menggunakan metode kuantitatif. Syahrizal dan Jailani sepakat bahwa metode penelitian kuantitatif memiliki beberapa jenis, antara lain survei, *ex post facto*, *policy research*, *action research*, evaluasi, dan eksperimen [11]. Mengetahui hal tersebut, maka perancangan sistem pemilah sampah organik dan anorganik di SMP Terpadu Al-Qudwah ini menggunakan metode kuantitatif dengan jenis eksperimental.

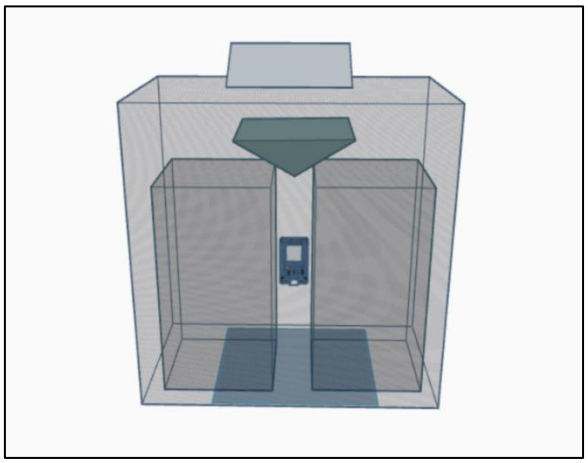
Metode eksperimen adalah metode penelitian yang digunakan untuk menjelaskan hubungan sebab-akibat antara variabel X dan variabel Y. Untuk memperoleh hasil yang valid, peneliti harus melakukan kontrol dan pengukuran variabel secara cermat. Penelitian eksperimen dapat dilakukan di lingkungan terbuka maupun di ruang tertutup, dan dalam prosesnya peneliti bebas memanipulasi kondisi sesuai kebutuhan penelitian [11].

Flowchart diawali dengan *state* mulai, proses oleh sensor, kemudian pemilahan sampah akan jatuh ke tong organik atau organik, lalu *display*, hingga proses manual pembuangan sampah oleh petugas kebersihan.



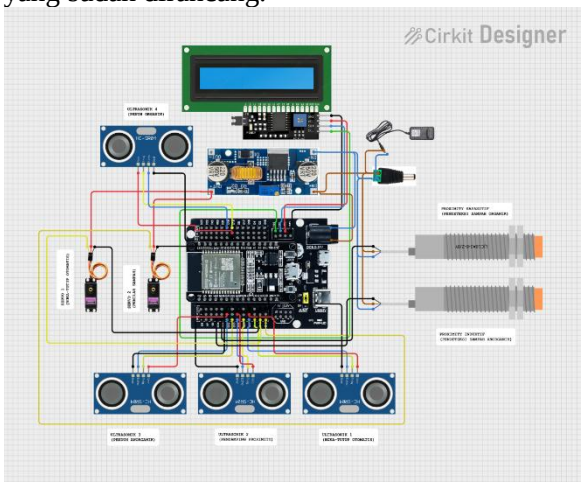
Gambar 7. *Flowchart Smart Bin*

Tahap pertama dalam perancangan tempat sampah pintar ini adalah desain bentuknya. Desain bentuk sistem dalam penelitian ini menggunakan *website* Tingkercad.



Gambar 8. Desain 3D Tempat Sampah Pintar

Tahap kedua yaitu desain pengkabelan atau *wiring* yang menggunakan *website* Cirkit Designer. Berikut sistem *wiring* seluruh komponen yang sudah dirancang.



Gambar 9. Wiring Keseluruhan Komponen

Teknik pengujian sistem *smart bin* menggunakan *black box testing*. Metode pengujiannya berfokus pada pemeriksaan fungsi sistem berdasarkan sudut pandang pengguna. Pada pengujian *black box testing* ini, penguji tidak mengetahui maupun memeriksa proses internal yang terjadi di dalam sistem, melainkan hanya menilai apakah sistem menghasilkan keluaran yang sesuai dengan yang diharapkan. Tujuan utama dari pengujian *black box* adalah memastikan bahwa seluruh fungsi sistem dapat berjalan dengan baik dan benar ketika digunakan oleh pengguna, dengan menilai hasil aktual yang dapat dilihat secara langsung tanpa memperhatikan mekanisme internal sistem tersebut [12].

Terkait Teknik pengumpulan data dilakukan dengan menyebar angket tingkat kepuasan siswa/i di SMP Terpadu Al-Qudwah terhadap tempat sampah pintar yang sudah dirancang. Angket atau kusioner ini memiliki 10 pertanyaan yang perlu dijawab “Ya” atau “Tidak.” Cara menjawabnya cukup mudah, hanya dengan memberi simbol *check list* di kolom “Ya” atau “Tidak.”

Kelas di SMP Terpadu Al-Qudwah terbagi sesuai jenis kelamin dan angka. Contohnya 7 Putra 1, 7 Putra 2, 7 Putra 3, 7 Putri 1, 7 Putri 2, dan seterusnya hingga kelas 9. Karena *smart bin* yang dirancang hanya 1 buah, maka untuk pengumpulan data diperlukan satu kelas saja untuk sampel.

Teknik *sampling* yang digunakan adalah *Cluster Random Sampling* atau *sampling* kluster merupakan teknik pengambilan sampel dengan cara membagi populasi ke dalam beberapa kelompok berdasarkan wilayah geografis atau unit administratif yang disebut kluster. Selanjutnya, beberapa kluster dipilih secara acak, dan data penelitian dikumpulkan dari seluruh atau sebagian anggota dalam kluster yang terpilih tersebut [13]. Pemilihannya menggunakan *website Wheel of Names* dan didapatkan kelas 9 Putri 1 yang berjumlah 20 siswi.

3. HASIL DAN PEMBAHASAN

3.1. Pembahasan

Sistem smart bin yang dirancang terdiri dari dua bagian utama, yaitu perangkat keras (*hardware*) dan perangkat lunak (*software*) yang saling terintegrasi. Perangkat keras berfungsi sebagai alat pendeteksi dan aktuator, sedangkan perangkat lunak berperan dalam pengolahan data sensor serta pengambilan keputusan. Mikrokontroler ESP32 digunakan sebagai pusat kendali sistem sekaligus penghubung dengan jaringan internet.

Fungsi utama dari sistem yang dirancang meliputi mekanisme buka-tutup tempat sampah secara otomatis, pemilahan sampah organik dan anorganik, serta pendeteksian kapasitas tempat sampah. Selain itu, sistem juga dilengkapi dengan fitur pengiriman notifikasi melalui bot Telegram apabila tempat sampah telah mencapai kondisi penuh. Seluruh fungsi tersebut dirancang untuk bekerja secara otomatis guna meminimalkan keterlibatan pengguna dalam proses pemilahan.

Sistem *smart bin* ini dibuat menggunakan triplek dan kayu reng, yang di dalamnya terdapat tempat sampah organik serta anorganik, lengkap dengan komponen pembantu untuk keberhasilan pemilahan limbah. Tempat sampah pintar ini memiliki dua buah pintu untuk mengosongkan tong yang sudah penuh dan pemeliharaan komponen di dalamnya. Kedua pintu tersebut dilengkapi dengan kunci grendel agar tertutup dan rapi. Kemudian di bagian atas *smart bin* terdapat sistem buka-tutup sebagai tempat masuk sampah, sensor ultrasonik untuk mendeteksi objek, dan LCD guna menampilkan pesan.

Gambar 10. *Smart Bin* Tampak Luar

Apabila sensor ultrasonik mendeteksi objek dan mekanisme buka-tutup otomatis bekerja, maka di dalamnya terlihat sebuah sistem pemilah. Terdapat sensor proximity kapasitif, induktif, dan ultrasonik untuk membantu memilah sampah organik dan anorganik. Apabila pintu tempat sampah pintar dibuka, maka akan terlihat di dalamnya terdapat 2 buah tong, 1 untuk limbah organik, dan 1 untuk anorganik. Tong yang dipakai mempunyai kapasitas 20 liter. Ketika pintu dibuka juga terlihat struktur kompartemen yang cukup kokoh. Selain itu, terlihat juga setiap koponen yang saling terhubung oleh kabel *jumper* dan terpusat di ESP32 dan *expansion*-nya. Dayanya diantar oleh adaptor 12V 2A lewat belakang melalui lubang yang sudah disiapkan.

Gambar 11. *Smart Bin* Tampak Dalam

3.2. Hasil

Hasil perancangan pada penelitian ini berupa sebuah tempat sampah pintar (*smart bin*) berbasis *Internet of Things* (IoT) yang dirancang untuk membantu proses pemilahan sampah organik dan anorganik secara otomatis. Sistem ini direncanakan untuk diterapkan di lingkungan SMP Terpadu Al-Qudwah, dengan tujuan mendukung kegiatan pemilahan sampah dan pengelolaan waste bank di sekolah.

Berdasarkan pengujian *black box*, sistem yang dikembangkan secara fungsional telah berjalan sebagaimana mestinya dan mampu menghasilkan keluaran yang sesuai. Hasil pengujian *black box* menunjukkan bahwa sistem pemilah sampah organik dan anorganik cukup berfungsi baik walaupun beberapa jenis limbah tidak sesuai dengan hasil yang diharapkan.

Tabel 1. *Black Box* Pengujian Sistem

No.	Nama Sampah	Gambar	Hasil		
			1	2	3
1.	Kulit buah pisang		Plastik/ Kertas	Organik	Organik
2.	Kaleng minuman		Logam	Plastik/ Kertas	Logam
3.	Kertas		Plastik/ Kertas	Plastik/ Kertas	Plastik/ Kertas

No.	Nama Sampah	Gambar	Hasil		
			1	2	3
4.	Daun		Plastik/ Kertas	Organik	Organik
5.	Timun		Organik	Plastik/ Kertas	Organik
6.	Tutup plastik		Plastik/ Kertas	Plastik/ Kertas	Plastik/ Kertas

Selain menyimpan tempat sampah pintar di kelas, dilakukan juga penyebaran angket atau kuesioner tingkat kepuasan. Kuesioner penelitian tersebut berisi 10 pertanyaan yang berkaitan dengan kepuasan para siswi terhadap sistem *smart bin* yang telah dirancang. Siswi hanya perlu melakukan *check list* di 10 pertanyaan tersebut, bisa diletakkan di “Ya” atau “Tidak.”

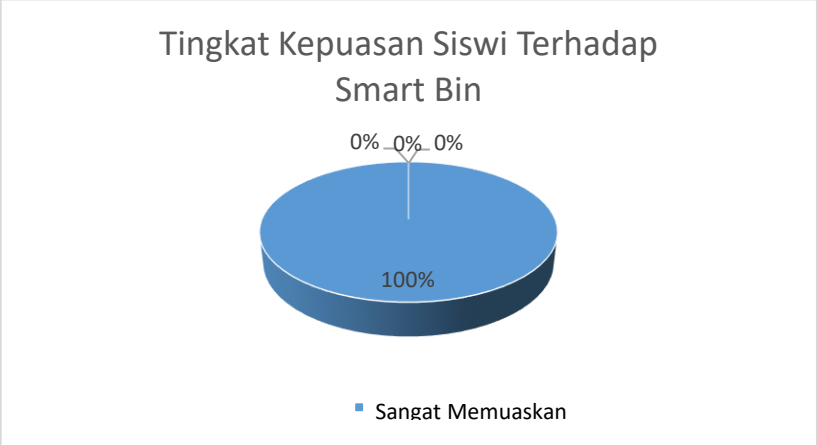
Data yang diperoleh kemudian diolah dalam bentuk tabel dan diagram, sehingga memudahkan untuk dipahami.

Tabel 2. Hasil Kuisioner Tingkat Kepuasan

No	Nama	Skor Total	Kategori
1	Aisha Azalea H	10	Sangat Memuaskan
2	Almira Carissa P.P	8	Sangat Memuaskan
3	Alya Yunisya	10	Sangat Memuaskan
4	Aura Kasinah Putri	10	Sangat Memuaskan
5	Balqis Al Khadni'ah	10	Sangat Memuaskan
6	Cila Hidayat	10	Sangat Memuaskan
7	Cinta Marchiana Arifin	10	Sangat Memuaskan
8	Gendis Farisa	10	Sangat Memuaskan
9	Gravitannisa	9	Sangat Memuaskan
10	Jayyida	10	Sangat Memuaskan
11	Jelita Fatimah Azzahra	10	Sangat Memuaskan
12	Kayyisa Najla Kamila	10	Sangat Memuaskan
13	Khansa A.Z	9	Sangat Memuaskan
14	Malika Rahma M.	10	Sangat Memuaskan

No	Nama	Skor Total	Kategori
15	Naela Sekar K	10	Sangat Memuaskan
16	Restiawati	10	Sangat Memuaskan
17	Saskia Nadiya Putri	10	Sangat Memuaskan
18	Shafa N.A	10	Sangat Memuaskan
19	Shafa Salsabila	10	Sangat Memuaskan
20	Syifa Alisa Zahra	10	Sangat Memuaskan

Sebanyak 20 siswi 9 Putri 1 di SMP Terpadu Al-Qudwah menyimpulkan bahwa *smart bin* yang dirancang cukup memuaskan. Skor tertinggi adalah 10, karena apabila menjawab "Ya" bernilai 1, sedangkan "Tidak" bernilai "0". Kategori yang digunakan adalah "Sangat Memuaskan", "Memuaskan", "Cukup Memuaskan", dan "Tidak Memuaskan". Nilai interval paling kecil adalah 2.5, hasil dari 4 kategori dibagi dengan jumlah pertanyaan. Kemudian setiap nilai kategori dijumlahkan dengan 2.5, hingga mencapai nilai tertinggi yaitu 10.



Grafik 1. Diagram Lingkaran Tingkat Kepuasan

4. KESIMPULAN

Berdasarkan hasil pengujian tempat sampah pintar pemilah limbah organik dan anorganik, ditemukan beberapa kesimpulan. Pertama, sampah organik sulit terdeteksi karena harus menyentuh sensor, sedangkan sampah anorganik mudah terdeteksi. Sampah kecil juga bisa terjebak dan tidak jatuh ke tong. Kedua, sistem buka-tutup otomatis dan pendeteksian tong penuh berfungsi baik, namun kabelnya mudah putus. Ketiga, sistem pendeteksi tong penuh dapat mengirim notifikasi lewat bot Telegram, tetapi tergantung koneksi Wi-Fi. Tempat sampah ini kurang akurat dan perlu perhatian pada sensor dan kabel.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih yang mendalam kepada berbagai pihak yang telah membantu dalam proses penulisan skripsi. Pertama, kepada Allah SWT yang selalu memenuhi harapan. Kedua, kepada orang tua, Bapak Ahmad Setia Budi dan Ibu Laila Sari, atas doa dan dukungan mereka. Penulis juga mengucapkan terima kasih kepada Bapak Dr. Pranoto, Bapak Dr. E. Nurzaman, Bapak Dr. Imam Sofi'i, dan penguji skripsi, Bapak Muhammad Fauzi serta Ibu Eva. Selain itu, ucapan terima kasih juga ditujukan kepada Kepala SMP Terpadu Al-Qudah dan siswi kelas 9, serta Zahra Nadhifah yang memberikan dukungan. Penulis menghargai teman-teman yang memberikan semangat dan bantuan serta berterima kasih kepada diri sendiri atas usaha yang telah dilakukan. Penulis berharap Allah SWT membalas kebaikan semua pihak.

DAFTAR PUSTAKA

[1] Z. Zuraidah, L. N. Rosyidah, and R. F. Zulfi, "EDUKASI PENGELOLAAN DAN PEMANFAATAN SAMPAH ANORGANIK DI MI AL MUNIR DESA GADUNGAN KECAMATAN PUNCU KABUPATEN KEDIRI," *BUDIMAS J. Pengabdi. Masy.*, vol. 4, no. 2, Oct. 2022, doi: 10.29040/budimas.v4i2.6547.

[2] A. Ibnul Rasidi, Y. A. H. Pasaribu, A. Ziqri, and F. D. Adhinata, "Klasifikasi Sampah Organik dan Non-Organik Menggunakan Convolutional Neural Network," *J. Tek. Inform. Dan Sist. Inf.*, vol. 8, no. 1, Apr. 2022, doi: 10.28932/jutisi.v8i1.4314.

[3] S. Wahyuningsih, B. Widiati, T. Melinda, and T. Abdullah, "Sosialisasi Pemilahan Sampah Organik dan Non-Organik Serta Pengadaan Tempat Sampah Organik dan Non-Organik," *Dedik. SAINTEK J. Pengabdi. Masy.*, vol. 2, no. 1, pp. 7–15, Apr. 2023, doi: 10.58545/djpm.v2i1.103.

[4] Wardah and R. R. Sihmawati, "Pengelolaan Sampah Organik Menjadi Nutrisi Probiotik dan KomposGuna Mendorong Pembangunan Berkelanjutan di Desa Pabean Kecamatan Sedati Sidoarjo," *J. Abdidas*, vol. 06, no. 03, pp. 238–248, 2025, doi: 10.31004/abdidas.v5i6.1075.

[5] B. A. Ramadhan, I. Rizianiza, and F. Manta, "Rancang Bangun Tempat Sampah Pemilah Otomatis Berbasis Arduino," *J. Rekayasa Mesin*, vol. 17, no. 2, p. 265, Aug. 2022, doi: 10.32497/jrm.v17i2.3283.

[6] D. Harianto, H. S. Bintang, A. Ardiyanto, and V. L. D. Widyawan, "Development and Evaluation of an ESP32-based Temperature and Humidity Control Unit for Textile Storage," *Int. J. Eng. Contin.*, vol. 4, no. 1, pp. 1–19, Nov. 2024, doi: 10.58291/ijec.v4i1.309.

[7] A. Ra'uf, A. Faisol, and F. Santi Wahyuni, "PENGGUNAAAN INTERNET OF THINGS (IOT) ALAT PENDETEKSI LOGAM DAN NON-LOGAM PADA TEMPAT SAMPAH PINTAR," *JATI J. Mhs. Tek. Inform.*, vol. 6, no. 2, pp. 1176–1183, Jan. 2023, doi: 10.36040/jati.v6i2.5398.

[8] R. S. Santoso, S. Qisti, M. Subito, T. S. Sollu, R. Fauzi, and E. Ardias, "RANCANG BANGUN TEMPAT SAMPAH OTOMATIS DENGAN PEMILAH SAMPAH ORGANIK DAN ANORGANIK DISERTAI NOTIFIKASI SMS BERBASIS ARDUINO," *Foristek*, vol. 14, no. 2, Nov. 2023, doi: 10.54757/fs.v14i2.323.

[9] M. Shaqis, N. Wahidah, N. Syawal, Sakrina, Nur'amalia, and F. S. Waruwu, "Mentoring Pembuatan Tempat Sampah Otomatis Berbasis Arduino di SMKN 3," *J. Lepa-Lepa Open*, vol. 1, no. 4, pp. 842–853, 2021, doi: https: //ojs.unm.ac.id/JLLO/index.

[10] A. S. Sumaedi, F. R. R. Ramdhani Rosman, and F. F. Fiqri, "Perancangan Sistem Keamanan Pendeteksi Gas dalam Ruangan menggunakan Sensor Gas Mq-2 Berbasis Mikrokontroler Arduino Uno R3," *J. SISKOM-KB Sist. Komput. Dan Kecerdasan Buatan*, vol. 7, no. 3, pp. 198–207, Jul. 2024, doi: 10.47970/siskom-kb.v7i3.675.

[11] H. Syahrizal and M. S. Jailani, "Jenis-Jenis Penelitian Dalam Penelitian Kuantitatif dan Kualitatif," *J. QOSIM J. Pendidik. Sos. Hum.*, vol. 1, no. 1, pp. 13–23, May 2023, doi: 10.61104/jq.v1i1.49.

[12] M. N. Muhammad, M. A. Nurdin, and H. Permatasari, "Pengujian Aplikasi Pengelolaan Laundry Menggunakan Metode Blackbox Testing dan Whitebox Testing," 2023.

[13] N. Trianasari, P. Kencana Sari, and A. Prasetio, "Peningkatan Kualitas Penelitian di Bidang Kesehatan Melalui Pelatihan Penentuan Teknik Sampling dan Besar Sampel di STFI Bandung," *J. Pengabdi. Masy. Pemberdaya. Inov. Dan Perubahan*, vol. 5, no. 1, pp. 348–355, Jan. 2025, doi: 10.59818/jpm.v5i2.1152.

Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Analisis Manajemen Risiko Berbasis ISO 31000 pada Aspek Operasional Teknologi Informasi PT. Schlumberger Geophysics Nusantara

[1]Yogi Kamal, [2*]Andi Al-Ghifari, [3]M Afdhal H, [4]Fajar
[1,2,3] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia
*Email: *[1]anditriarusman@gmail.com*
(Naskah masuk: 3 Juni 2026, diterima untuk diterbitkan: 31 Juli 2026)

Abstrak: *PT. Schlumberger Geophysics Nusantara merupakan perusahaan multinasional terkemuka di bidang teknologi dan jasa terintegrasi untuk industri minyak dan gas bumi, berlokasi di Wisma Mulia Suite 45th Floor, Jakarta Selatan. Perusahaan ini mengandalkan platform DELFI berbasis cloud untuk mengelola seluruh kegiatan operasionalnya. Ketergantungan tinggi terhadap sistem teknologi informasi (TI) menimbulkan berbagai risiko operasional yang perlu dikelola secara sistematis. Penelitian ini menganalisis manajemen risiko operasional TI menggunakan kerangka kerja ISO 31000:2009 melalui pendekatan kualitatif deskriptif. Data dikumpulkan melalui wawancara terstruktur dengan Project Manager dan Account Manager Divisi Digital & Integration. Penilaian risiko menggunakan matriks likelihood × impact skala 1–5. Hasil penelitian mengidentifikasi 14 risiko operasional TI: 11 risiko (78,57%) pada tingkat Tinggi (skor ≥15) dan 3 risiko (21,43%) pada tingkat Menengah. Risiko tertinggi meliputi downtime sistem DELFI, serangan siber, dan kebocoran data. ISO 31000 terbukti mampu memberikan gambaran terstruktur mengenai tingkat risiko dan prioritas penanganannya untuk mendukung keberlanjutan operasional TI perusahaan.*

Kata Kunci – *Manajemen Risiko; ISO 31000; Teknologi Informasi; Risiko Operasional; Keamanan Siber*

Abstract: *PT. Schlumberger Geophysics Nusantara is a leading multinational company in integrated technology and services for the oil and gas industry, located at Wisma Mulia Suite 45th Floor, South Jakarta. The company relies on the cloud-based DELFI platform to manage all its operational activities. High dependence on information technology (IT) systems creates various operational risks that require systematic management. This study analyzes IT operational risk management using the ISO 31000:2009 framework through a qualitative descriptive approach. Data was collected through structured interviews with the Project Manager and Account Manager of the Digital & Integration Division. Risk assessment uses a likelihood × impact matrix on a 1–5 scale. The study identified 14 IT operational risks: 11 risks (78.57%) at High level (score ≥15) and 3 risks (21.43%) at Moderate level. The highest risks include DELFI system downtime, cyber attacks, and data breaches. ISO 31000 proved effective in providing a structured overview of risk levels and handling priorities to support the sustainability of the company's IT operations.*

Keywords – *Risk Management; ISO 31000; Information Technology; Operational Risk; Cybersecurity*

Pendahuluan

PT. Schlumberger Geophysics Nusantara merupakan perusahaan multinasional nomor satu di dunia di bidang penyediaan teknologi informasi dan jasa terintegrasi untuk industri minyak dan gas bumi. Perusahaan ini berlokasi di Wisma Mulia Suite 45th Floor, Jl. Jend. Gatot Subroto Kav. 42, Jakarta Selatan. Perusahaan menyediakan solusi teknologi canggih untuk kegiatan karakterisasi, pengeboran, produksi, dan pengolahan reservoir, serta bergerak di bidang konsultasi dan manajemen proyek terintegrasi [1].

Platform DELFI merupakan inovasi utama perusahaan, yaitu sistem penyimpanan dan pengelolaan data berbasis cloud yang mendukung seluruh kegiatan operasional dan penjualan. Ketergantungan tinggi terhadap sistem TI berbasis cloud membawa konsekuensi berupa meningkatnya eksposur risiko operasional [2]. Berbagai ancaman seperti downtime sistem, serangan siber, kehilangan

Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666
P-ISSN : 3031-2779
E-ISSN : 3026-4197

data, gangguan jaringan, kerusakan hardware, serta human error berpotensi mengganggu kelangsungan bisnis secara signifikan.

Penelitian sebelumnya oleh Manuputty et al. [5] pada perusahaan yang sama mengidentifikasi 14 risiko operasional TI dengan 11 risiko di level High dan 3 risiko di level Moderate, membuktikan tingginya kerentanan TI perusahaan. Penelitian ini hadir sebagai pembaruan dengan metode wawancara langsung kepada narasumber kunci. ISO 31000:2009 dipilih sebagai kerangka karena bersifat generik, fleksibel, dan tidak mensyaratkan sertifikasi [4]. Penelitian Atmojo & Manuputty [6], Kuncoro et al. [7], serta Herlambang et al. [8] juga membuktikan efektivitas ISO 31000 dalam analisis risiko TI berbagai organisasi.

Penelitian ini bertujuan: (1) mengidentifikasi seluruh risiko operasional TI PT. Schlumberger Geophysics Nusantara; (2) menganalisis tingkat kemungkinan dan dampak setiap risiko; (3) mengevaluasi tingkat dan prioritas risiko; serta (4) merumuskan usulan perlakuan risiko yang dapat diimplementasikan perusahaan.

Metode Penelitian

2.1 Jenis dan Pendekatan Penelitian

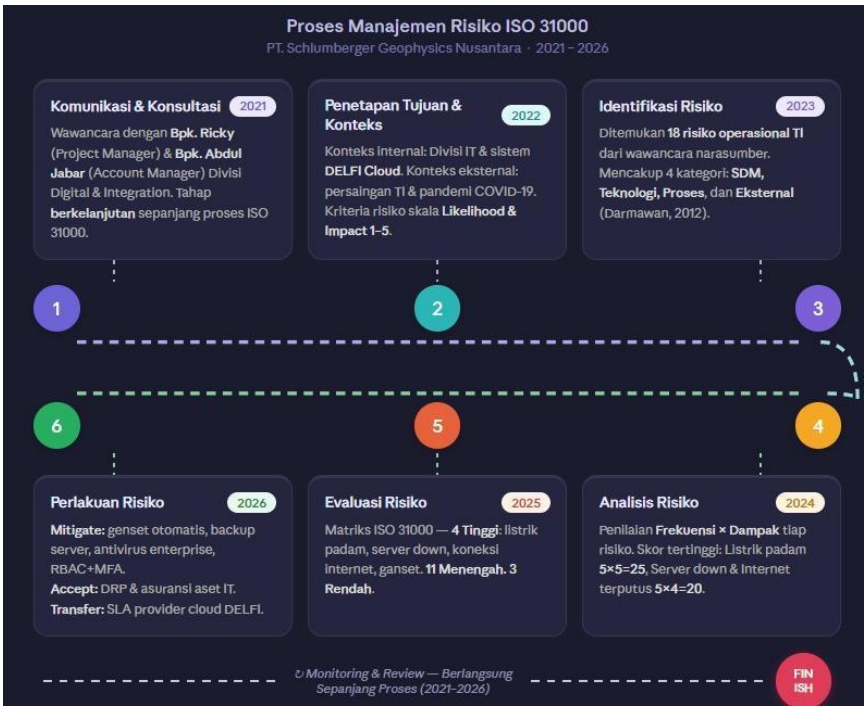
Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan mengadopsi kerangka kerja ISO 31000:2009 sebagai metode utama analisis risiko. Objek penelitian adalah aspek operasional teknologi informasi PT. Schlumberger Geophysics Nusantara, khususnya yang berkaitan dengan platform DELFI berbasis cloud. Pendekatan kualitatif dipilih karena penelitian ini berfokus pada eksplorasi mendalam terhadap kondisi aktual risiko operasional TI perusahaan [13].

2.2 Teknik Pengumpulan Data

Data primer diperoleh melalui wawancara terstruktur yang dilaksanakan pada 7 Mei 2026. Narasumber terdiri dari: (1) Project Manager PT. Schlumberger Geophysics Nusantara; dan (2) Account Manager Divisi Digital & Integration. Pemilihan narasumber dilakukan secara purposive karena keduanya memiliki pengetahuan langsung mengenai kondisi risiko operasional TI perusahaan.

2.3 Tahapan Analisis ISO 31000

Proses analisis risiko mengikuti tahapan ISO 31000:2009 seperti ditunjukkan pada Gambar 1.

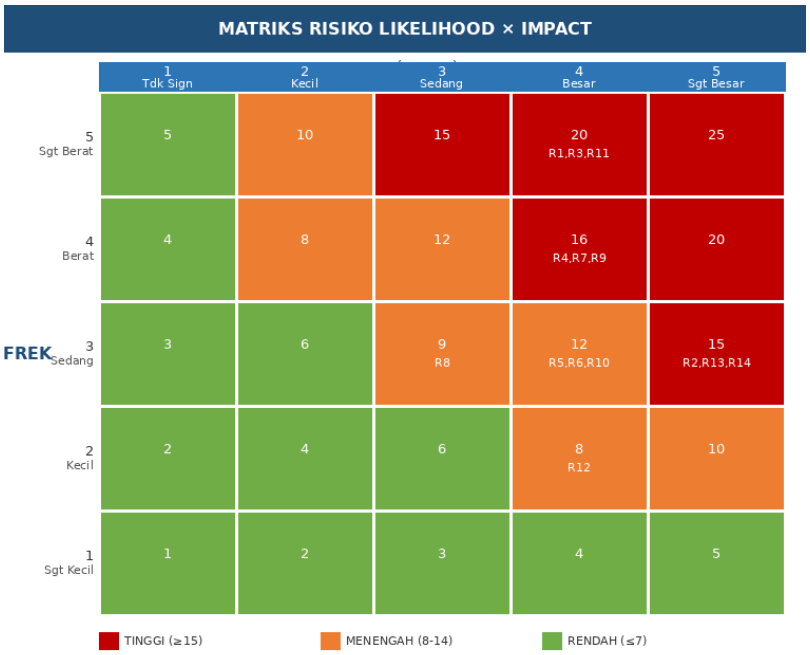


Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Gambar 1. Alur Proses Manajemen Risiko ISO 31000:2009

Tingkat risiko ditentukan dari skor Frekuensi (F) × Dampak (D) menggunakan skala 1–5 dengan kategori: Rendah (≤7), Menengah (8–14), dan Tinggi (≥15). Matriks penilaian risiko 5×5 ditunjukkan pada Gambar 2.



Gambar 2. Matriks Risiko Likelihood × Impact 5×5

Hasil dan Pembahasan

3.1 Penetapan Konteks

Penetapan konteks internal mencakup struktur Divisi IT perusahaan yang terdiri dari Project Manager, IT Development, IT Operations, IT Network & Infrastructure, dan Account Manager Divisi Digital & Integration. Perusahaan memiliki ketergantungan sangat tinggi terhadap platform DELFI berbasis cloud untuk seluruh kegiatan operasional harian di sektor minyak dan gas.

Penetapan konteks eksternal mencakup: (1) persaingan ketat antar penyedia teknologi informasi di industri energi global; (2) perkembangan teknologi digital yang pesat; (3) ancaman keamanan siber global yang terus meningkat; serta (4) regulasi pemerintah Indonesia terkait pengelolaan data dan cloud computing (PP No. 71/2019).

3.2 Identifikasi Risiko

Berdasarkan hasil wawancara dan analisis konteks, diperoleh 14 risiko operasional TI yang dikelompokkan ke dalam 4 kategori sebagaimana disajikan pada Tabel 1.

Tabel 1. Identifikasi Risiko Operasional TI PT. Schlumberger Geophysics Nusantara

No	Kode	Kemungkinan Risiko	Kategori
1	**R1**	Downtime / kegagalan sistem DELFI	Risiko Teknologi
2	**R2**	Kehilangan atau korupsi data perusahaan	Risiko Teknologi
3	**R3**	Serangan siber (hacking, malware, ransomware)	Risiko Eksternal
4	**R4**	Gangguan koneksi internet / jaringan	Risiko Teknologi
5	**R5**	Kesalahan konfigurasi sistem cloud	Risiko Proses

Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666
P-ISSN : 3031-2779
E-ISSN : 3026-4197

No	Kode	Kemungkinan Risiko	Kategori
6	**R6**	Kerusakan hardware (server, storage)	Risiko Teknologi
7	**R7**	Human error oleh operator TI	Risiko SDM
8	**R8**	Kurangnya kompetensi / pelatihan SDM TI	Risiko SDM
9	**R9**	Gangguan pasokan listrik / kegagalan UPS	Risiko Teknologi
10	**R10**	Ketergantungan berlebihan pada penyedia cloud	Risiko Eksternal
11	**R11**	Kebocoran data / pelanggaran keamanan data	Risiko Eksternal
12	**R12**	Perubahan regulasi pemerintah terkait data dan cloud	Risiko Eksternal
13	**R13**	Kegagalan sistem backup dan disaster recovery	Risiko Proses
14	**R14**	Serangan Distributed Denial of Service (DDoS)	Risiko Eksternal

3.3 Analisis dan Evaluasi Risiko

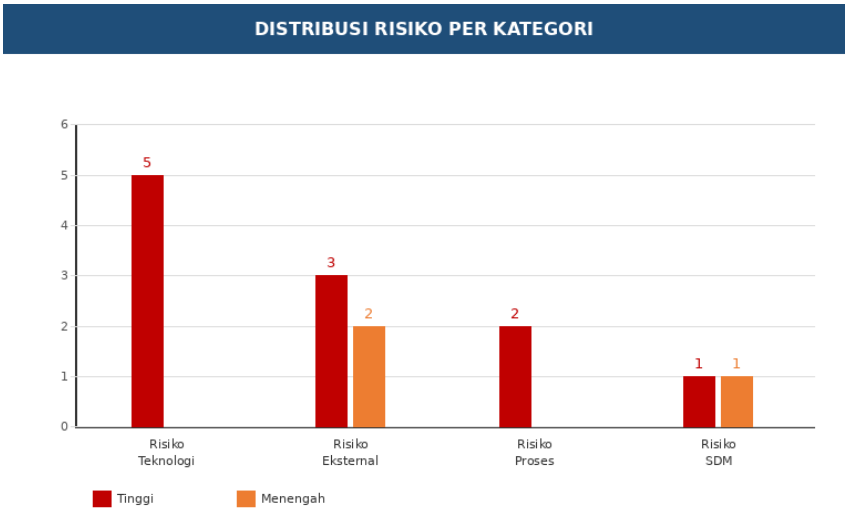
Hasil analisis dan evaluasi 14 risiko operasional TI berdasarkan penilaian F×D disajikan pada Tabel 2.

Tabel 2. Hasil Analisis dan Evaluasi Risiko Operasional TI

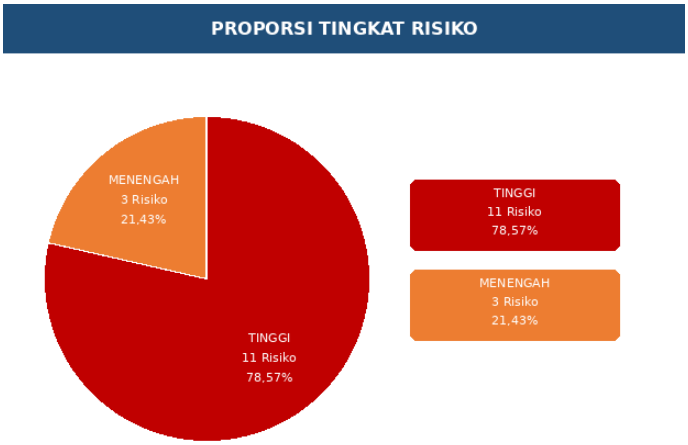
Kode	Kemungkinan Risiko	F	D	F×D	Level	Tindakan
R1	Downtime / kegagalan sistem DELFI	4	5	**20**	**Tinggi**	Segera
R2	Kehilangan atau korupsi data	3	5	**15**	**Tinggi**	Segera
R3	Serangan siber	4	5	**20**	**Tinggi**	Segera
R4	Gangguan koneksi jaringan	4	4	**16**	**Tinggi**	Segera
R5	Kesalahan konfigurasi cloud	3	4	**12**	**Tinggi**	Segera
R6	Kerusakan hardware	3	4	**12**	**Tinggi**	Segera
R7	Human error operator TI	4	4	**16**	**Tinggi**	Segera
R8	Kurangnya kompetensi SDM TI	3	3	**9**	**Menengah**	Direncanakan
R9	Gangguan listrik / kegagalan UPS	4	4	**16**	**Tinggi**	Segera
R10	Ketergantungan penyedia cloud	3	4	**12**	**Tinggi**	Segera
R11	Kebocoran data	4	5	**20**	**Tinggi**	Segera
R12	Perubahan regulasi data dan cloud	2	4	**8**	**Menengah**	Direncanakan
R13	Kegagalan sistem backup	3	5	**15**	**Tinggi**	Segera
R14	Serangan DDoS	3	5	**15**	**Tinggi**	Segera

Distribusi risiko per kategori ditunjukkan pada Gambar 3 dan proporsi tingkat risiko pada Gambar 4

Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666
P-ISSN : 3031-2779
E-ISSN : 3026-4197



Gambar 3. Distribusi Risiko Operasional TI per Kategori



Gambar 4. Proporsi Tingkat Risiko Operasional TI

Berdasarkan Gambar 3 dan Gambar 4, Risiko Teknologi mendominasi dengan 5 risiko tingkat Tinggi (R1, R2, R4, R6, R9), diikuti Risiko Eksternal dengan 3 risiko Tinggi dan 2 Menengah. Secara keseluruhan, 78,57% risiko berada pada level Tinggi. Risiko dengan skor tertinggi (F×D = 20) adalah R1, R3, dan R11 yang menjadi prioritas utama. Temuan ini konsisten dengan penelitian Manuputty et al. [5] pada perusahaan yang sama.

3.4 Pengendalian / Perlakuan Risiko

Seluruh 11 risiko tingkat Tinggi memerlukan penanganan segera, sedangkan 3 risiko Menengah direncanakan secara berkala. Tabel 3 menyajikan usulan perlakuan risiko secara lengkap.

Tabel 3. Usulan Perlakuan Risiko Operasional TI

Kode	Level	Risiko	Usulan Perlakuan Risiko
R1	**Tinggi**	Downtime sistem DELFI	Menerapkan redundansi server (failover), monitoring real-time 24/7, serta menyusun dan menguji Disaster Recovery Plan (DRP) minimal setiap 6 bulan.
R2	**Tinggi**	Kehilangan/korupsi data	Backup otomatis harian dengan multi-location storage, enkripsi data end-to-end, dan asuransi data penting perusahaan.
R3	**Tinggi**	Serangan siber	Implementasi firewall, IDS/IPS, enkripsi end-to-end, dan pelatihan anti-phishing rutin setiap 3 bulan.
R4	**Tinggi**	Gangguan koneksi jaringan	Multi-ISP dengan automatic failover, peningkatan bandwidth, dan koneksi backup VPN/dedicated line.

Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666
P-ISSN : 3031-2779
E-ISSN : 3026-4197

Kode	Level	Risiko	Usulan Perlakuan Risiko
R5	**Tinggi**	Kesalahan konfigurasi cloud	Standar konfigurasi cloud (hardening guide) dan double approval oleh tim senior sebelum perubahan diterapkan.
R6	**Tinggi**	Kerusakan hardware	Preventive maintenance bulanan, hardware redundancy (RAID, dual power), dan spare part kritis di gudang.
R7	**Tinggi**	Human error operator	SOP operasional detail, pelatihan rutin, double-check approval aktivitas kritis, dan audit log terpusat.
R8	**Menengah**	Kurangnya kompetensi SDM	Program sertifikasi tahunan (CompTIA, CISSP, AWS) dan knowledge sharing internal bulanan.
R9	**Tinggi**	Gangguan listrik/UPS	Peningkatan kapasitas UPS, generator cadangan dengan ATS, dan pemeliharaan perangkat listrik setiap 3 bulan.
R10	**Tinggi**	Ketergantungan cloud vendor	Negosiasi SLA (uptime 99,99%), implementasi multi-cloud strategy, dan contingency plan gangguan vendor.
R11	**Tinggi**	Kebocoran data	RBAC, DLP, audit log berkala, enkripsi database, dan compliance PP No. 71/2019.
R12	**Menengah**	Perubahan regulasi	Monitoring regulasi per kuartal dan penyesuaian kebijakan internal sesuai perubahan regulasi.
R13	**Tinggi**	Kegagalan sistem backup	Pengujian backup dan recovery setiap 3 bulan, dokumentasi hasil, dan backup offsite/cloud terenkripsi.
R14	**Tinggi**	Serangan DDoS	DDoS protection berbasis cloud (Cloudflare/AWS Shield), peningkatan bandwidth, dan prosedur respons insiden DDoS.

Kesimpulan

Berdasarkan analisis manajemen risiko operasional TI pada PT. Schlumberger Geophysics Nusantara menggunakan kerangka kerja ISO 31000:2009, diperoleh kesimpulan sebagai berikut:

1. Teridentifikasi 14 risiko operasional TI yang terbagi dalam 4 kategori: Teknologi (5 risiko Tinggi), Eksternal (3 risiko Tinggi, 2 Menengah), Proses (2 risiko Tinggi), dan SDM (1 risiko Tinggi, 1 Menengah). Tingginya proporsi risiko pada kategori Teknologi dan Eksternal mencerminkan kerentanan inheren dari model operasional berbasis cloud yang diadopsi perusahaan.
2. Dari total 14 risiko, 11 risiko (78,57%) berada pada tingkat Tinggi dengan skor $F \times D \geq 15$, dan 3 risiko (21,43%) pada tingkat Menengah dengan skor F×D antara 8–14. Distribusi ini konsisten dengan temuan Manuputty et al. [5] dan mengonfirmasi bahwa perusahaan berbasis platform cloud tunggal menghadapi eksposur risiko yang lebih tinggi dibandingkan perusahaan dengan infrastruktur hybrid.
3. Risiko dengan skor tertinggi ($F \times D = 20$) adalah downtime sistem DELFI (R1), serangan siber (R3), dan kebocoran data (R11), yang ketiganya menjadi prioritas utama penanganan segera. Ketiga risiko ini saling berkaitan karena kegagalan pada satu aspek dapat memicu kaskade risiko pada aspek lainnya.
4. Usulan perlakuan risiko yang dirumuskan mengikuti empat pendekatan ISO 31000: penghindaran, pengurangan, pemindahan, dan penerimaan risiko. Implementasi diprioritaskan dalam dua tahap: jangka pendek (0–3 bulan) untuk risiko skor 20, dan jangka menengah (3–6 bulan) untuk risiko skor 12–16.
5. Kerangka kerja ISO 31000:2009 terbukti efektif memberikan gambaran terstruktur mengenai tingkat risiko dan prioritas penanganannya untuk mendukung keberlanjutan operasional TI perusahaan berbasis cloud. Penelitian lanjutan disarankan melibatkan lebih banyak narasumber lintas divisi dan mengintegrasikan metode kuantitatif seperti simulasi Monte Carlo untuk estimasi risiko yang lebih presisi.

Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm. 93-99
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada PT. Schlumberger Geophysics Nusantara, khususnya kepada Bapak/Ibu Project Manager dan Account Manager Divisi Digital & Integration yang telah meluangkan waktu dan bersedia memberikan informasi serta data yang diperlukan dalam penelitian ini. Apresiasi juga disampaikan kepada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, [Universitas Muslim Indonesia] atas dukungan akademik yang diberikan selama proses penelitian berlangsung.

Daftar Pustaka

[1] R.R. Moeller, Brink's Modern Internal Auditing: A Common Body of Knowledge, 8th ed. Hoboken: Wiley, 2016.

[2] I. Grey, S. Manson, dan L. Crawford, The Audit Process: Principles, Practice and Cases, 6th ed. Cengage Learning, 2015.

[3] N.M. Sirait dan A. Susanty, "Analisis risiko operasional berdasarkan pendekatan Enterprise Risk Management (ERM) pada CV Mitra Dunia Palletindo," Industrial Engineering Online Journal, vol. 5, no. 4, 2016.

[4] International Organization for Standardization, ISO 31000:2009 Risk Management — Principles and Guidelines. Geneva: ISO, 2009.

[5] G.P. Manuputty, A. Abdul Azis, dan N.A. Nur Pratami, "Analisis manajemen risiko berbasis ISO 31000 pada aspek operasional teknologi informasi PT. Schlumberger Geophysics Nusantara," E-Prosiding Akuntansi Universitas Trilogi, 2022. https://trilogi.ac.id/journal/ks/index.php/EPAKT/article/view/1171

[6] S.A. Atmojo dan A.D. Manuputty, "Analisis manajemen risiko teknologi informasi menggunakan ISO 31000 pada aplikasi AHO Office," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 7, no. 3, hal. 546–558, 2020.

[7] S.D. Kuncoro, R.A. Ghaisan, M.U. Zaky, dan A. Wulansari, "Manajemen risiko pada teknologi informasi: Studi kasus pada perusahaan jasa," Prosiding Seminar Nasional Informatika, vol. 1, hal. 313–323, 2023.

[8] A.A. Herlambang, A.A. Gani, dan D.D. Alvianto, "Pendekatan ISO 31000:2018 dalam manajemen risiko teknologi informasi pada Tracer Study Universitas Sebelas April," Jurnal Teknologi Informasi dan Komunikasi, hal. 5651–5660, 2024.

[9] Jericho dan E. Haryani, "Penerapan ISO 31000:2018 dalam manajemen risiko teknologi informasi pada sistem penerbitan PT. X," Jurnal Informasi, Sains dan Teknologi (ISAINTEK), vol. 7, no. 2, 2024. https://isaintek.polinef.ac.id/index.php/isaintek/article/view/269

[10] A.M. Siregar et al., "Standarisasi manajemen risiko ISO 31000: Tantangan dan strategi implementasi pada PT. Telkom Indonesia," JERKIN: Jurnal Ekonomi, Riset, Kajian dan Inovasi, 2025. https://jerkin.org/index.php/jerkin/article/view/1564

[11] N. Safaat H, "Manajemen risiko teknologi informasi menggunakan framework ISO 31000 studi kasus sistem infrastruktur TI Telkom Indonesia," SITEKIN: Jurnal Sains, Teknologi dan Industri, vol. 12, no. 2, 2015.

[12] B. Prasetyo, A. Salsabila, dan W.E.Y. Retnani, "IT risk management analysis based on ISO 31000 and Bow Tie Analysis in higher education institution," Indonesian Journal of Information Systems, vol. 7, no. 1, hal. 84–96, 2024. https://doi.org/10.24002/ijis.v7i1.9673

[13] Iswajuni, A. Manasikana, dan S. Soetedjo, "The effect of enterprise risk management on firm value in manufacturing companies listed on Indonesian Stock Exchange," Asian Journal of Accounting Research, vol. 3, no. 2, hal. 224–236, 2018.

[14] H.A.M. Hani, D.R.I. Indah, dan P.E.S. Putri, "Analisis manajemen risiko pada teknologi informasi PT. Pos Indonesia menggunakan ISO 31000," Indonesian Journal of Computer Science, vol. 12, no. 6, hal. 3957–3974, 2023. https://doi.org/10.33022/ijcs.v12i6.3504

[15] S.D. Mulyati, R.A. Kuncoro, dan A. Wulansari, "Optimalisasi manajemen risiko teknologi informasi menggunakan framework ISO 31000 di era digital," JISAMAR, vol. 9, no. 1, 2025. https://journal.stmikjayakarta.ac.id/index.php/jisamar/article/view/1690

Jicom : Journal Information & Computer
Volume 4, Nomor 2, Juli 2026, hlm.100-109
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Sistem Pakar Diagnosa Penyakit Ispa Menggunakan Metode *Certainty Factor*

Lona Monika Sinabutar[1], Nadya Tiara Utami[2], Novita Dwiyanti Manullang[3], Anita Desiani[4], Endang Sri Kresnawati[5]

[1,2,3,4,5] Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sriwijaya
Email: [*1]08011282328073@student.unsri.ac.id, [2]08011282328049@student.unsri.ac.id,
[3]08011282328053@student.unsri.ac.id, [4]anita_desiani@unsri.ac.id, [5]eskresna@unsri.ac.id

(Naskah masuk: *4 Juni 2026*, diterima untuk diterbitkan: *31 Juli 2026*)

Abstrak: *Gangguan pernapasan merupakan salah satu masalah kesehatan yang dapat berdampak serius jika tidak dideteksi dan ditangani dengan baik. Salah satu penyakit gangguan pernapasan yang umum terjadi adalah Infeksi Saluran Pernapasan Akut (ISPA). Infeksi saluran pernapasan disebabkan oleh virus. Penyakit ISPA mempunyai banyak jenis seperti Sinusitis, Pneumonia, Faringitis, Common cold, Bronchitis, Asma, Pertusis, dan Epiglotitis. Penyakit ISPA termasuk dalam kategori penyakit dengan angka kejadian yang tinggi dan dapat berakibat fatal jika tidak ditangani dengan tepat. Oleh karena itu, diperlukan suatu sistem yang dapat membantu dalam mendeteksi dan mendiagnosis Penyakit ISPA secara dini, salah satunya adalah sistem pakar. Penelitian ini merancang sistem pakar yang menggunakan metode Certainty Factor (CF), metode ini dapat mempermudah mendiagnosa penyakit ISPA. Metode ini memiliki keunggulan dalam menangani ketidakpastian, khususnya dalam mendiagnosis penyakit berdasarkan gejala yang diberikan.*
Kata Kunci – *Sistem Pakar; Certainty Factor; Infeksi Saluran Pernapasan Akut (ISPA); Diagnosis Penyakit Gangguan Pernapasan.*

Abstract: *Respiratory disorders are one of the health problems that can have serious consequences if not properly detected and treated. One of the most common respiratory diseases is Acute Respiratory Infection (ARI). According to data from WHO, ARI is classified as a disease with a high incidence rate and can be fatal if not treated appropriately. Therefore, a system that can assist in the early detection and diagnosis of ARI is needed, one of which is an expert system. An expert system is an artificial intelligence-based system capable of mimicking an expert's reasoning process in analyzing a disease. One of the methods used in expert systems is the Certainty Factor method. This method has the advantage of handling uncertainty, particularly in diagnosing diseases based on given symptoms. This study discusses the application of the Certainty Factor method in an expert system for diagnosing ARI to support a more accurate and efficient diagnostic process.*
Keywords – *Expert System; Certainty Factor; Acute Respiratory Infection (ARI); Disease Diagnosis; Respiratory Disorders.*

1. PENDAHULUAN

Ilmu pengetahun dan teknologi berkembang maju di setiap aspek kegiatan manusia. Seluruh kegiatan manusia kini berhubungan erat dengan peranan teknologi khususnya komputer. Pada bidang kesehatan kini sangat memanfaatkan kemajuan teknologi dalam peningkatan pelayanan kesehatan. Selama ini, proses diagnosa penyakit pasien sangat bergantung kepada dokter dengan cara yang masih manual[1]. Salah satu penyakit yang memiliki tingkat jumlah kasus yang tinggi dan masih banyak dianggap remeh adalah penyakit Infeksi Saluran Pernapasan Akut (ISPA)[2].

ISPA atau Infeksi Saluran Pernapasan Akut merupakan salah satu gangguan pernapasan yang sering terjadi dan dapat disebabkan oleh virus, bakteri, serta jamur. ISPA sangat mudah menular melalui udara dengan didukung faktor lingkungan seperti polusi udara, asap rokok, serta kebersihan lingkungan yang kurang baik[3]. ISPA menjadi permasalahan serius di berbagai negara. Berdasarkan informasi dari WHO (*World Health*

Organization), ISPA menjadi penyebab utama morbiditas dan mortalitas penyakit menular di dunia dengan hampir empat juta kematian setiap tahun[4]. Berdasarkan data dari Kementrian Kesehatan, ISPA juga menjadi kasus penyakit yang paling sering ditangani di Indonesia dengan angka mencapai 1,5 hingga 1,8 juta kasus[5].

Berdasarkan pertimbangan di atas maka diperlukanlah sebuah sistem pakar yang dapat mendiagnosa penyakit ISPA dalam pemanfaatan teknologi dibidang kesehatan. Sistem pakar bekerja dengan menggunakan basis pengetahuan dan aturan tertentu yang memungkinkan pengguna mendapatkan solusi atas suatu permasalahan tanpa perlu berkonsultasi langsung dengan ahli berbasis komputer[6]. Fungsi utama sistem pakar adalah memberikan rekomendasi atau keputusan berdasarkan data yang diberikan, serta membantu dalam analisis suatu masalah dengan tingkat akurasi yang tinggi[7]. Manfaat dari sistem ini antara lain meningkatkan efisiensi dalam proses diagnosis, mengurangi beban kerja tenaga medis, serta memberikan kemudahan akses bagi masyarakat dalam memperoleh informasi kesehatan yang valid[8]. Salah satu metode yang digunakan dalam proses penarikan kesimpulan pada sistem pakar adalah metode *Certainty Factor*. Metode ini diterapkan untuk menangani permasalahan yang memiliki tingkat kepastian yang tidak mutlak[9]. *Certainty Factor* berfungsi sebagai ukuran kepercayaan terhadap suatu fakta, yang mencerminkan tingkat keyakinan seorang pakar dalam menyelesaikan suatu permasalahan**.**

Beberapa jurnal penelitian mengenai pemanfaatan sistem pakar untuk diagnosa awal penyakit ISPA sudah banyak dilakukan. Jurnal penelitian pertama berjudul Sistem Pakar Diagnosa Penyakit ISPA berbasis web dengan metode *Forward Chaining*. Penelitian tersebut menggunakan metode *Forward Chaining*, dari hasil penelitian tertinggi yaitu mampu mendiagnosis penyakit epiglotitis 80 %[10]. Jurnal selanjutnya berjudul Sistem pakar diagnosis penyakit Infeksi Saluran Pernapasan Akut (ISPA) menggunakan metode *Dempster Shafer*. Penelitian tersebut menggunakan metode *Dempster Shafer*, dari hasil penelitian tertinggi yaitu mampu mendiagnosis penyakit *common cold* 90%[11].

Dengan adanya kemajuan teknologi dan kecerdasan buatan, penerapan sistem pakar dalam bidang kesehatan dapat menjadi solusi efektif dalam mengatasi permasalahan diagnosis dini penyakit. Oleh karena itu, penelitian ini akan mengembangkan dan mengimplementasikan sistem pakar berbasis *Certainty Factor* guna memberikan diagnosa awal terhadap penyakit gangguan pernapasan secara lebih cepat, akurat, dan dapat diakses oleh masyarakat luas[12]**.**

Penelitian ini bertujuan untuk menerapkan metode *Certainty Factor* dalam sistem pakar untuk mendiagnosis penyakit gangguan pernapasan. Dengan adanya sistem pakar, diharapkan masyarakat dapat memperoleh informasi awal mengenai kemungkinan penyakit yang mereka derita berdasarkan gejala yang mereka alami. Selain itu, sistem pakar juga dapat menjadi alat bantu bagi tenaga medis dalam mempercepat proses diagnosis dan memberikan rekomendasi tindakan yang lebih tepat bagi pasien[13]**.**

2. METODE PENELITIAN

2.1. Pengumpulan Data

Pengumpulan data menggunakan beberapa literatur dari seorang ahli atau pakar untuk menentukan gejala dan penyakit ISPA. Berdasarkan hasil pengumpulan data ini, didapatkan 38 gejala penyakit ISPA dengan 8 jenis penyakit ini antara lain sinusitis, Pneumonia, faringitis, commond cold, bronkitis, asma, pertussis, epiglottitis[5]. Jenis penyakit ISPA tersebut kemudian diberi kode pada masing-masing penyakit yang dapat dilihat pada tabel 1.

Tabel 1. Jenis Penyakit

Kode Penyakit	Nama Penyakit
A	Sinusitis
B	Pneumonia
C	Faringitis
D	Common Cold
E	Bronkitis
F	Asma
G	Pertussis

H	Epiglottitis

Setiap jenis penyakit memiliki sejumlah gejala yang dialami. Dengan demikian, satu jenis penyakit dapat memunculkan lebih dari satu gejala, baik yang serupa maupun yang berbeda. Gejala-gejala penyakit Infeksi Saluran Pernapasan Akut (ISPA) bersumber dari penelitian yang dilakukan oleh Puput dkk [5] dan M.Afdhal dkk[6]. Terdapat 38 gejala yang terkait dengan penyakit ISPA. Setiap gejala tersebut telah diberi label yang dapat dilihat pada Tabel 2.

Tabel 2. Data Gejala Penyakit ISPA

Kode Gejala	Gejala-Gejala
G01	Tekanan atau rasa sakit/nyeri di area wajah
G02	Hidung tersumbat atau pilek
G03	Pusing atau sakit kepala
G04	Batuk
G05	Hilangnya indra penciuman dan indera perasa
G06	Demam rendah
G07	Bau mulut (halitosis)
G08	Sakit tenggorokan
G09	Diare
G10	Demam tinggi
G11	Kesulitan bernapas (napas pendek)
G12	Nyeri dada yang memburuk saat bernapas dalam
G13	Kehilangan nafsu makan
G14	Kelelahan dan rasa sakit tubuh secara umum
G15	Mual dan muntah
G16	Pembengkakan kelenjar getah bening
G17	Kemerahan dan pembengkakan
G18	Sulit menelan
G19	Batuk kering atau batuk dengan dahak ringan
G20	Suara serak atau hilangnya suara
G21	Nyeri telinga atau tekanan pada telinga
G22	Sesak nafas atau kesulitan bernafas
G23	Frekuensi Pernafasan cepat
G24	Mengi (mengeluarkan suara saat bernafas)
G25	Peningkatan denyut jantung
G26	Bersin bersin
G27	Tenggorokan gatal
G28	Badan terasa lemas
G29	Nyeri saat menelan
G30	Batuk berdahak
G31	Lendir kental kuning dari hidung
G32	Sianosis atau tubuh menjadi sedikit membiru
G33	Selalu dehidrasi
G34	Batuk berdahak disertai darah
G35	Linglung atau terjadi penurunan kesadaran
G36	Drooling atau air liur keluar berlebihan
G37	Muntah akibat rejan parah
G38	Sakit atau rasa tidak nyaman pada dada

Selanjutnya, terdapat aturan yang disusun dalam bentuk pernyataan IF [asumsikan] THEN [kesimpulan]. Gejala yang diinputkan serta kesimpulan yang dihasilkan akan berpengaruh terhadap jenis penyakit Infeksi Saluran Pernapasan Akut (ISPA). Dengan demikian, pola pernyataannya adalah IF (gejala) THEN (jenis penyakit ISPA). Setiap jenis penyakit memiliki berbagai gejala; oleh karena itu, untuk menghubungkan beberapa gejala dalam satu aturan, digunakan operator logika AND [dan], yang dapat dilihat pada Tabel 3.

Tabel 3. Aturan (Rule) CF

Penyakit	Logika Aturan (*Rule*)
Sinusitis[A]	IF G01 AND G02 AND G03 AND G04 AND G05 AND G06 AND G07 AND G08 AND G11 AND G28 AND G30 AND G31 AND G35 AND G38 THEN A
Pneumonia [B]	IF G04 AND G08 AND G09 AND G10 AND G11 AND G12 AND G13 AND G14 AND G15 AND G28 AND G34 THEN B
Faringitis [C]	IF G03 AND G04 AND G06 AND G07 AND G08 AND G14 AND G15 AND G16 AND G17 AND G18 AND G19 AND G20 AND G21 AND G27 AND G28 AND G13 AND G29 THEN C
Commond Cold/Batuk Pilek [D]	IF G26 AND G02 AND G20 AND G05 AND G17 AND G03 AND G30 AND G06 AND G04 THEN D
Bronchitis [E]	IF G02 AND G03 AND G22 AND G28 AND G30 AND G35 AND G38 THEN E
Asma [F]	IF G04 AND G14 AND G22 AND G23 AND G24 AND G25 AND G38 THEN F
Pertusis (Batuk rejan) [G]	IF G02 AND G04 AND G06 AND G22 AND G24 AND G28 AND G32 AND G37 THEN G
Epiglotitis [H]	IF G06 AND G08 AND G20 AND G22 AND G24 AND G29 AND G32 AND G36 THEN H

Selanjutnya, sistem pakar ini memerlukan pembobotan yang mencakup tingkat keyakinan pengguna terhadap gejala penyakit serta bobot dari gejala tersebut untuk menentukan jenis penyakit yang diderita. Pengguna akan memasukkan pilihan dari angka 1 hingga 6 sebagai respons terhadap tingkat keyakinan terhadap gejala yang dirasakan. Tingkat keyakinan ini berkisar dari tingkat keyakinan yang tinggi (pasti) hingga tingkat keyakinan yang rendah (tidak), sebagaimana diuraikan dalam Tabel 4.

Tabel 4. Nilai CF User

No	Keterangan	Nilai User
1	Pasti	1
2	Hampir Pasti	0.8
3	Kemungkinan Besar	0.6
4	Mungkin	0.4
5	Tidak tahu	0.2
6	Tidak	0

Tingkat keyakinan pengguna terhadap gejala penyakit memiliki bobot yang bervariasi. Bobot tersebut mencerminkan tingkat keyakinan pengguna mengenai setiap gejala penyakit yang disajikan oleh sistem. Semakin tinggi nilai bobot yang diberikan, semakin tinggi pula tingkat keyakinan pengguna tersebut. Oleh

karena itu, diagnosis terhadap jenis penyakit juga dipengaruhi oleh bobot gejala yang dipilih oleh pengguna sistem. Nilai bobot masing-masing gejala untuk setiap jenis penyakit Infeksi Saluran Pernapasan Akut (ISPA) dapat dilihat pada Tabel 5.

Tabel 5. Nilai Bobot Gejala pada Penyakit ISPA

Jenis Penyakit	Nama Gejala	Bobot
Sinusitis	Tekanan atau rasa sakit di area wajah	0.10
	Hidung tersumbat atau pilek	0.26
	Pusing atau sakit kepala	0.24
	Batuk	0.34
	Hilangnya indra penciuman dan indra perasa	0.90
	Demam rendah	0.40
	Bau mulut (halitosis)	0.20
	Sakit tenggorokan	0.22
	Badan terasa lemas	0.18
	Kesulitan bernapas (napas pendek)	0.80
	Batuk berdahak	0.28
	Linglung atau terjadi Penurunan kesadaran	0.16
	Sakit atau rasa tidak nyaman pada dada	0.26
	Lendir kental kuning dari hidung	0.10
Pneumonia	Batuk	0.34
	Sakit tenggorokan	0.22
	Diare	0.40
	Demam tinggi	0.60
	Kesulitan Bernapas (napas pendek)	0.80
	Nyeri dada yang memburuk saat bernapas dalam	0.40
	Kehilangan nafsu makan	0.20
	Kelelahan dan rasa sakit tubuh secara umum	0.40
	Mual dan muntah	0.20
	Badan terasa lemas	0.18
	Batuk berdahak disertai darah	0.10
Faringitis	Pusing atau sakit kepala	0.24
	Batuk	0.34
	Demam rendah	0.40
	Bau mulut (halitosis)	0.20
	Sakit tenggrokan	0.22
	Kelelahan dan rasa sakit tubuh secara umum	0.40
	Mual dan muntah	0.20
	Pembengkakan kelenjar getah bening	0.40
	Sulit menelan	0.80
	Kemerahan dan pembengkakan	0.80
	Batuk kering atau batuk dengan dahak ringan	0.40
	Suara serak atau hilangnya suara	0.28
	Nyeri telinga atau tekanan pada telinga	0.60
	Tenggorokan gatal	0.28
	Badan terasa lemas	0.18
	Kehilangan nafsu makan	0.20
	Nyeri saat menelan	0.10
	Bersin bersin	0.80
	Hidung tersumbat atau pilek	0.26

Jenis Penyakit	Nama Gejala	Bobot
Commond cold/Batuk pilek	Hilangnya indra penciuman dan indra perasa	0.90
	Suara serak atau hilangnya suara	0.28
	Tenggorokan gatal	0.28
	Pusing atau sakit kepala	0.24
	Demam rendah	0.40
	Batuk berdahak	0.28
	Batuk	0.34
Bronchitis	Hidung tersumbat atau pilek	0.26
	Pusing atau sakit kepala	0.24
	Sesak nafas atau kesulitan bernafas	0.40
	Badan terasa lemas	0.18
	Batuk berdahak	0.28
	Linglung atau terjadi penurunan kesadaran	0.16
	Sakit atau rasa tidak nyaman pada dada	0.26
Asma	Batuk	0.34
	Kelelahan dan rasa sakit tubuh secara umum	0.40
	Sesak nafas atau kesulitan bernafas	0.40
	Frekuensi pernafasan cepat	0.24
	Mengi (mengeluarkan suara saat bernafas)	0.22
	Peningkatan denyut jantung	0.40
	Sakit atau rasa tidak nyaman pada dada	0.26
Pertusis (Batuk rejan)	Hidung tersumbat atau pilek	0.26
	Batuk	0.34
	Demam rendah	0.40
	Sesak nafas atau kesulitan bernafas	0.40
	Mengi (mengeluarkan suara saat bernafas)	0.22
	Badan terasa lemas	0.18
	Sianosis atau tubuh menjadi sedikit membiru	0.26
	Muntah akibat rejan yang parah	0.10
Epiglotitis	Demam rendah	0.40
	Sakit tenggorokan	0.22
	Suara serak atau hilangnya suara	0.41
	Sesak nafas atau kesulitan bernafas	0.40
	Mengi (mengeluarkan suara saat bernafas)	0.22
	Nyeri saat menelan	0.10
	Sianosis atau tubuh menjadi sedikit membiru	0.26
	Drooling atau air liur keluar berlebihan	0.10

2.2. Perancangan Sistem Pakar

Pada tahap perancangan sistem pakar ini menggunakan metode certainty factor. Berdasarkan penilaian pakar, metode certainty factor menunjukkan tingkat keyakinan terhadap suatu kejadian. Kemudian, dalam mengasumsikan derajat kepastian seorang ahli atau pakar pada data digunakan suatu nilai tertentu pada metode certainty factor[14]. Berikut rumus Certainty Factor dapat dilihat pada persamaan persamaan 1, 2, 3, 4 dan 5 [15].

$$CF[h,e] = MB[h,e] - MD[h,e] \quad (1)$$

Keterangan:

$CF[h,e]$ = faktor kepastian (*certainty factor*)

$MB[h,e]$ = ukuran kepastian (*measure of belief*) terhadap hipotesis (h) jika diberikan *evidence* (e) antara 0 dan 1

$MD[h,e]$ = ukuran ketidakpastian (*measure of disbelief*) terhadap hipotesis (h) jika diberikan *evidence* (e) antara 0 dan 1

h = hipotesis

e = fakta (*evidence*)

Adapun rumus beberapa kombinasi dari *certainty factor* terhadap suatu premis tertentu sebagai berikut:

1. Rumus *certainty factor* untuk aturan premis tunggal

$$CF[h,e] = CF * CF[e] = CF[user] * CF[pakar] \quad (2)$$

2. Rumus *certainty factor* untuk lebih dari satu premis

$$CF[A \wedge B] = Min(CF[a], CF[b]) * CF[rule] \quad (3)$$

$$CF[A \vee B] = Max(CF[a], CF[b]) * CF[rule] \quad (4)$$

3. Rumus *certainty factor* untuk kesimpulan yang serupa

$$CF_{gabungan} = [CF1, CF2] = CF1 + CF2 * 1(1 - CF1) \quad (5)$$

3. HASIL DAN PEMBAHASAN

3.1. Pembahasan

Untuk menguji sistem pakar dengan metode certainty factor dalam mendiagnosa penyakit ISPA digunakan nilai CF gejala, bobot kepercayaan, serta bobot pengaruh gejala terhadap jenis penyakit ISPA yang dipilih oleh pasien. Gejala-Gejala yang dirasakan oleh pasien tersebut akan diuji pada sistem pakar ini guna melihat tingkat akurasi dari sistem apakah sesuai dengan penyakit yang diderita oleh pasien. Setelah data uji disiapkan, maka data tersebut masuk tahap perhitungan nilai CF gejala dan nilai CF pengguna, sistem melanjutkan proses dengan menentukan nilai CF kombinasi untuk setiap jenis penyakit. Selanjutnya nilai CF kombinasi akan dikali dengan 100% untuk menampilkan hasil diagnose dalam bentuk persentase. Jawaban pasien dapat dilihat pada Tabel 6.

Tabel 6. Jawaban Pasien

Kode Gejala	Gejala-Gejala	Pasien 1	Pasien 2	Pasien 3
G01	Tekanan atau rasa sakit/nyeri di area wajah	6	4	5
G02	Hidung tersumbat atau pilek	6	1	4
G03	Pusing atau sakit kepala	6	4	6
G04	Batuk	6	3	6
G05	Hilangnya indra penciuman dan indra perasa	6	5	2
G06	Demam rendah	6	3	6
G07	Bau mulut (halitosis)	6	3	6
G08	Sakit tenggorokan	6	1	6
G09	Diare	6	4	5
G10	Demam tinggi	6	5	3
G11	Kesulitan bernapas (napas pendek)	6	4	1

Kode Gejala	Gejala-Gejala	Pasien 1	Pasien 2	Pasien 3
G12	Nyeri dada yang memburuk saat bernapas dalam	4	1	4
G13	Kehilangan nafsu makan	6	1	6
G14	Kelelahan dan rasa sakit tubuh secara umum	2	5	2
G15	Mual dan muntah	3	2	3
G16	Pembengkakan kelenjar getah bening	6	2	6
G17	Kemerahan dan pembengkakan	6	3	6
G18	Sulit menelan	6	2	6
G19	Batuk kering atau batuk dengan dahak ringan	6	1	6
G20	Suara serak atau hilangnya suara	6	5	6
G21	Nyeri telinga atau tekanan pada telinga	5	4	5
G22	Sesak nafas atau kesulitan bernafas	2	1	2
G23	Frekuensi Pernafasan cepat	6	3	6
G24	Mengi (mengeluarkan suara saat bernafas)	6	2	6
G25	Peningkatan denyut jantung	5	5	5
G26	Bersin bersin	6	3	6
G27	Tenggorokan gatal	6	1	6
G28	Badan terasa lemas	6	5	6
G29	Nyeri saat menelan	6	5	6
G30	Batuk berdahak	6	2	6
G31	Lendir kental kuning dari hidung	6	1	6
G32	Sianosis atau tubuh menjadi sedikit membiru	6	1	2
G33	Selalu dehidrasi	6	5	5
G34	Batuk berdahak disertai darah	6	4	6
G35	Linglung atau terjadi penurunan kesadaran	6	1	6
G36	Drooling atau air liur keluar berlebihan	6	3	6
G37	Muntah akibat rejan parah	6	5	4
G38	Sakit atau rasa tidak nyaman pada dada	6	3	3

Setelah dilakukan perhitungan CF kombinasi dan dikali 100%, perhitungan tersebut dilakukan serupa untuk semua jenis penyakit yang diperlihatkan pada Tabel 8. Berdasarkan Tabel 5, hasil perhitungan akurasi untuk masing-masing jenis penyakit terhadap kedua pasien dinyatakan dalam bentuk persentase, dimana akurasi yang akan menjadi variabel diagnosa dari sistem pakar adalah akurasi yang memiliki persentase tertinggi dan positif.

Tabel 8. Hasil Akurasi

Penyakit	Pasien 1	Pasien 2
Sinusitis	0%	92.9026%
Pneumonia	49.7344%	89.2864%
Faringitis	42.5336%	99.135%
Commond cold	0%	93.4267%
Bronkitis	0%	78.7131%
Asma	84.544%	75.9351%
Pertusis	0%	84.5271%
Epiglotitis	0%	81/1399%

4. KESIMPULAN

Sistem pakar dapat digunakan sebagai solusi dalam mendiagnosa penyakit ISPA, dengan menginputkan nilai kepastian *certainty factor* terhadap gejala yang dirasakan oleh pengguna sistem. Sistem pakar yang dirancang menggunakan metode *certainty factor* dalam mendiagnosa penyakit ISPA, terdapat 38

gejala dengan 8 jenis penyakit antara lain penyakit Sinusitis, Pneumonia, Faringitis, Common cold, Bronkitis, Asma, Pertusis dan Epiglottitis. Penelitian ini menggunakan data yang diambil dari seorang pasien penderita penyakit ISPA. Pasien sebagai pengguna sistem akan menginputkan nilai keyakinan terhadap gejala-gejala yang ditampilkan oleh sistem. Diagnosa penyakit ditetapkan dengan akurasi penyakit yang memiliki persentase tertinggi dibandingkan penyakit lainnya. Berdasarkan gejala yang dirasakan oleh pasien menghasilkan akurasi prediksi untuk setiap jenis penyakit Asma dimana sebesar 84.544%. Penerapan metode *certainty factor* efektif dalam pada sistem pakar diagnosa penyakit ISPA.

DAFTAR PUSTAKA

[1] Isy Karima Fauzia, Budi Arif Dermawan, and Tesa Nur Padilah, "Penerapan K-Means Clustering pada Penyakit Infeksi Saluran Pernapasan Akut (ISPA) di Kabupaten Karawang," *J. Sist. dan Inform.*, vol. 15, no. 1, pp. 81–87, 2020.

[2] D. D. Kusumaningtyas, M. Hasbi, and H. Wijayanto, "Sistem Pakar Diagnosa Penyakit Saluran Pernafasan Dengan Metode Fuzzy Tsukamoto," *J. Teknol. Inf. dan Komun.*, vol. 7, no. 2, pp. 1–7, 2019.

[3] M. Pieszka, D. Bederska-łojewska, P. Szczurek, and M. Pieszka, "The Membrane Interactions of Nano-Silica and Its Potential Application in Animal Nutrition," *Animals*, vol. 9, no. 12, pp. 1–13, 2019.

[4] J. Dhayanithi and M. P. Brundha, "Pencegahan dan pengendalian infeksi saluran pernapasan akut (ISPA) yang cenderung menjadi epidemi dan pandemi di fasilitas pelayanan kesehatan," in *Indian Journal of Forensic Medicine and Toxicology*, vol. 14, no. 4, 2007, pp. 4906–4911.

[5] P. D. Mandiri, D. Hartanti, and A. A. Sari, "Prototipe Sistem Pakar Untuk Diagnosis Penyakit Infeksi Saluran Pernapasan (Ispa) Menggunakan Metode Certainty Factor," *SKANIKA Sist. Komput. dan Tek. Inform.*, vol. 7, no. 2, pp. 180–191, 2024.

[6] M. Afdhal and Rita, "Sistem Pakar Diagnosa Penyakit ISPA dengan Menggunakan Metode Certainty Factor Berbasis Web," *J. Sist. Inf. dan Teknol. Inf.*, vol. 11, no. 2, pp. 133–139, 2022.

[7] A. Akmal and A. Pranolo, "Sistem Pakar Rekomendasi Obat Non-Resep Dokter dengan Metode Fuzzy Inference System Tsukamoto Berbasis Mobile Android," *JSTIE (Jurnal Sarj. Tek. Inform.*, vol. 7, no. 2, p. 56, 2019.

[8] C. Dian and P. Putra, "Sistem Pakar Diagnosa Penyakit Ispa (Infeksi Saluran Pernafasan Akut) Menggunakan Metode Certainty Factor Berbasis Web" *J. Mhs. Tek. Inform.*, vol. 1, no. 1, 2017, [Online].

[9] Asiva Noor Rachmayani, "Analisis Perbandingan Metode Certainty Factor, Dempster Shafer dan Teorema Bayes dalam Deteksi Dini," *J. Pendidik. dan Teknol. Indones.*, vol. 2, pp. 329–339, 2022.

[10] Karimah, Z. I. Nikmah, S. K. Aditya, and Elyza Gusti Wahyuni, "Aplikasi Web Untuk Pendeteksi Penyakit Paru-Paru Menggunakan Metode Certainty Factor," *J. Tek. Inform. Univ. Islam Indones.*, pp. 86–91, 2019.

[11] T. F. Ramadhani, I. Fitri, and E. T. E. Handayani, "Sistem Pakar Diagnosa Penyakit ISPA Berbasis Web dengan Metode Forward Chaining," *Jounal Inf. Technol. Comput. Sci.*, vol. 7, no. 1, pp. 738–746, 2022.

[12] M. T. Hidayatuloh and T. N. Suharsono, "Sistem Pakar Diagnosis Penyakit Infeksi Saluran Pernapasan Akut (ISPA) Menggunakan Metode Dempster Shafer," *Digit. Transform. Technol.*, vol. 3, no. 2, pp. 489–498, 2023.

[13] L. Septiana, "Perancangan Sistem Pakar Diagnosa Penyakit Ispa Dengan Metode Certainty Factor Berbasis Android," *J. TECHNO Nusa Mandiri*, vol. 13, no. 2, pp. 89–95, 2016.

[14] M. Iqbal, F. A. Setyaningsih, and S. Bahri, "Implementasi Metode Certainty Factor Dalam Sistem

Pakar Diagnosis Penyakit Paru-Paru Berbasis Android," *Coding J. Komput. dan Apl.*, vol. 7, no. 03, 2019.

[15] D. Abdurahman and Nunu Nurdiana, "Perancangan metode Certainty Factor untuk diagnosa Gagal Ginjal Kronis," *INFOTECH J.*, vol. 7, no. 2, pp. 1–8, 2021.

Jicom : Journal Information & Computer
Volume 4, Nomor 2, Juli 2026, hlm.110-117
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Implementasi Sistem Kunci Pintar 2FA Berbasis IoT Menggunakan RFID dan Bot Telegram pada ESP32

Syahrul Rozikin*[1], Muhammad Gald Teary[2], Fery Antony[3]
1,2,3,) Sistem Komputer, Fakultas Ilmu Komputer dan Sains, Universitas Indo Global Mandiri
Email: *[1]syahrulrozikin2704@gmail.com, [2]m.gald@uigm.ac.id, [3]feryantony@uigm.ac.id

(Naskah masuk: 7 Juni 2026, diterima untuk diterbitkan: 31 Juli 2026)

Abstrak: *Penelitian ini merancang dan mengimplementasikan prototipe sistem kunci pintar tanpa kunci (smart keyless) dengan autentikasi dua faktor berbasis Internet of Things (IoT) menggunakan ESP32, RFID RC522, bot Telegram, relay, dan solenoid lock 12V. Sistem membatasi akses fisik melalui dua tahap autentikasi, yaitu validasi UID kartu RFID dan OTP yang dikirim melalui bot Telegram. Pengujian dilakukan pada tiga skenario, yaitu RFID terdaftar dengan OTP valid, RFID terdaftar dengan OTP tidak valid, dan RFID tidak terdaftar. Hasil pengujian menunjukkan bahwa sistem bekerja sesuai rancangan dengan tingkat keberhasilan 100% dari 10 percobaan pada setiap skenario dalam kondisi pengujian prototipe terbatas. Waktu respons rata-rata aktivasi solenoid lock setelah autentikasi valid adalah 0,26 detik. Prototipe mampu menjalankan fungsi autentikasi dua tahap sesuai skenario uji, tetapi pengujian keamanan lanjutan masih diperlukan sebelum diterapkan pada lingkungan nyata.*
Kata Kunci *- kunci pintar; autentikasi dua faktor; RFID; bot Telegram; ESP32*

Abstract: *This study designs and implements a smart keyless prototype with two-factor authentication based on the Internet of Things (IoT) using ESP32, RFID RC522, Telegram bot, relay, and a 12V solenoid lock. The system restricts physical access through two authentication stages: validating the RFID card UID and verifying a one-time password (OTP) sent through the Telegram bot. Testing was conducted in three scenarios: registered RFID with valid OTP, registered RFID with invalid OTP, and unregistered RFID. The results show that the system worked according to the design, achieving 100% success in 10 trials for each scenario under limited prototype testing conditions. The average solenoid activation response time after valid authentication was 0.26 seconds. The prototype can perform basic two-factor authentication according to the tested scenarios, although further security testing is required before deployment in real operational environments.*
Keywords *- smart keyless; two-factor authentication; RFID; Telegram bot; ESP32*

1. PENDAHULUAN

Perkembangan Internet of Things (IoT) mendorong pemanfaatan perangkat tertanam untuk membangun sistem akses fisik yang dapat dikendalikan dan dipantau secara digital. Pada sistem pengamanan pintu, konsep kunci pintar tanpa kunci atau smart keyless memungkinkan proses pembukaan kunci dilakukan tanpa kunci mekanis konvensional, melainkan melalui media autentikasi elektronik seperti kartu RFID, perangkat bergerak, atau kode verifikasi sekali pakai. Namun, penggunaan RFID pada sistem akses tetap perlu memperhatikan aspek keamanan karena teknologi RFID masih memiliki risiko seperti penyalahgunaan kartu, pelacakan, replay attack, dan autentikasi yang lemah apabila hanya menggunakan satu faktor pengenal [1], [2].

Autentikasi merupakan aspek penting dalam sistem IoT karena perangkat yang terhubung ke jaringan dapat berinteraksi dengan pengguna, layanan komunikasi, dan aktuator fisik. Pada sistem akses berbasis RFID, kartu digunakan sebagai faktor kepemilikan untuk mengenali pengguna yang memiliki hak akses. Meskipun demikian, penggunaan RFID sebagai satu-satunya faktor autentikasi masih memiliki keterbatasan, misalnya ketika kartu hilang, dipinjamkan, atau digunakan oleh pihak yang tidak berwenang. Oleh karena itu, two-factor authentication (2FA) dapat digunakan sebagai lapisan tambahan dengan menggabungkan faktor kepemilikan berupa kartu RFID dan faktor verifikasi tambahan berupa kode OTP yang dikirim secara dinamis [3], [4].

Beberapa penelitian sebelumnya telah membahas sistem keamanan pintu berbasis RFID dan IoT. [5] merancang sistem keamanan ruang server berbasis RFID dan IoT untuk membatasi akses pada ruang server. [6] mengembangkan RFID smart door lock system berbasis IoT untuk manajemen membership fitness center. [7] mengembangkan smart home IoT dengan integrasi kunci RFID dan otomasi elektronik. [8] merancang sistem keamanan pintu berbasis RFID dan IoT, sedangkan [9] mengembangkan sistem keamanan pintu otomatis berbasis IoT dengan RFID, aplikasi mobile, dan metode Fuzzy Mamdani.

Penelitian lain mulai mengarah pada sistem autentikasi berlapis. [10] mengembangkan sistem keamanan loker dua lapis menggunakan RFID e-KTP dan OTP melalui platform Blynk. [11] membahas simulasi sistem keamanan dan kendali

gerbang otomatis berbasis IoT dengan teknologi tanpa kunci. [12] mengembangkan smart lock system berbasis IoT menggunakan ESP32 untuk keamanan akses pusat data. Selain itu, [13] menunjukkan penerapan mikrokontroler NodeMCU ESP8266 dan platform IoT ThingSpeak untuk pemantauan ruang server berbasis WiFi. Berdasarkan penelitian-penelitian tersebut, sistem akses berbasis RFID dan IoT telah banyak dikembangkan, tetapi masih terdapat ruang kajian pada penerapan autentikasi dua tahap yang menggabungkan UID RFID dan OTP melalui bot Telegram pada prototipe berbasis ESP32.

Research gap dalam penelitian ini terletak pada perlunya rancangan dan pengujian fungsional sistem smart keyless yang tidak hanya menunjukkan kondisi ketika akses diberikan, tetapi juga menjelaskan kondisi ketika akses harus ditolak, seperti kartu RFID tidak terdaftar, OTP salah, atau OTP tidak sesuai dengan proses autentikasi. Dengan demikian, penelitian ini tidak hanya berfokus pada keberhasilan membuka kunci, tetapi juga pada validasi logika autentikasi dua faktor dalam lingkup prototipe.

Tujuan penelitian ini adalah merancang, mengimplementasikan, dan menguji fungsi dasar sistem smart keyless 2FA berbasis RFID dan bot Telegram pada ESP32. Pengujian difokuskan pada validasi skenario akses, meliputi kartu RFID terdaftar dengan OTP valid, kartu RFID terdaftar dengan OTP tidak valid, serta kartu RFID tidak terdaftar. Fokus pengujian tersebut digunakan untuk memastikan bahwa sistem memberikan respons sesuai dengan kondisi autentikasi yang dirancang.

Kontribusi penelitian ini meliputi penyusunan arsitektur sistem smart keyless berbasis ESP32, perumusan alur autentikasi dua tahap menggunakan UID RFID dan OTP Telegram, implementasi pengendalian relay dan solenoid lock berdasarkan hasil autentikasi, serta pengujian fungsional terhadap beberapa skenario akses. Kontribusi tersebut diarahkan sebagai pembanding bagi penelitian sistem akses fisik berbasis IoT yang menerapkan autentikasi berlapis pada perangkat berbiaya relatif rendah.

Manfaat penelitian ini adalah memberikan referensi rancangan prototipe sistem akses fisik berbasis IoT yang menerapkan autentikasi dua tahap menggunakan RFID dan OTP Telegram. Secara praktis, hasil penelitian ini dapat digunakan sebagai dasar pengembangan sistem smart keyless sederhana untuk lingkungan terbatas, seperti laboratorium, ruang kerja, ruang penyimpanan, atau area dengan kebutuhan akses terbatas. Secara akademik, penelitian ini dapat menjadi bahan pembanding bagi penelitian berikutnya yang membahas integrasi RFID, ESP32, bot Telegram, dan mekanisme OTP pada sistem keamanan akses. Namun, manfaat tersebut tetap berada dalam ruang lingkup prototipe dan pengujian fungsional, sehingga belum dapat digeneralisasi sebagai sistem keamanan final tanpa pengujian lebih lanjut terhadap aspek jaringan, ketahanan perangkat, keamanan token, risiko penyalahgunaan kartu, dan skenario serangan lainnya.

2. METODE PENELITIAN

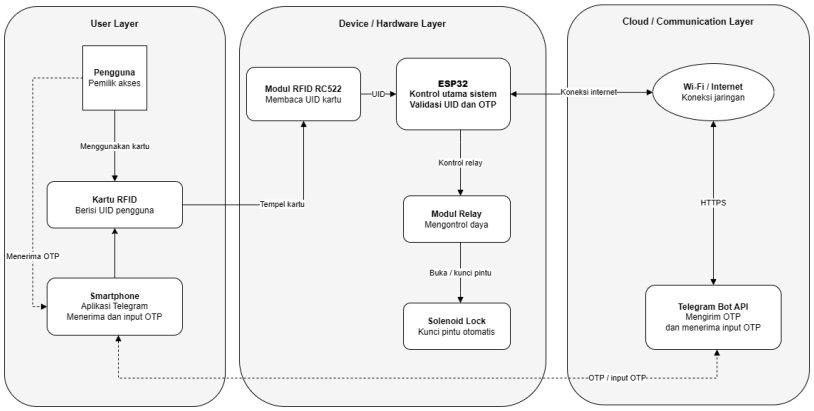
Penelitian ini menggunakan metode eksperimen berbasis prototipe untuk merancang dan menguji sistem smart keyless dengan autentikasi dua faktor berbasis Internet of Things (IoT). Sistem dikembangkan menggunakan ESP32 sebagai pengendali utama, RFID RC522 sebagai media autentikasi tahap pertama, Telegram Bot sebagai media pengiriman dan validasi One-Time Password (OTP), relay sebagai pengendali aktuator, serta solenoid lock 12V sebagai mekanisme penguncian.

Pengujian difokuskan pada fungsi autentikasi sistem berdasarkan kombinasi UID RFID dan OTP. Oleh karena itu, penelitian ini tidak bertujuan untuk menyatakan bahwa sistem telah sepenuhnya aman terhadap seluruh bentuk serangan, melainkan untuk menguji apakah sistem dapat memberikan respons sesuai dengan alur autentikasi yang dirancang.

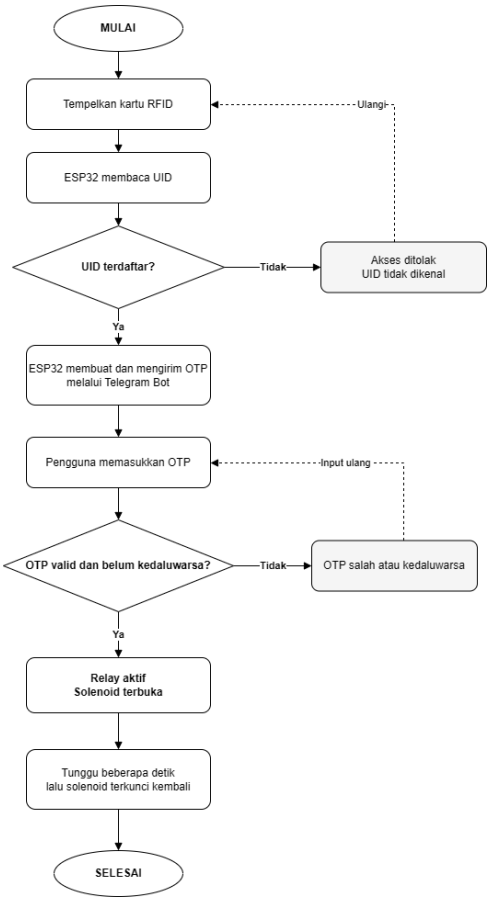
2.1. Desain Sistem

Sistem dirancang dengan alur autentikasi dua tahap. Tahap pertama dilakukan melalui pembacaan UID kartu RFID menggunakan modul RFID RC522. UID yang terbaca kemudian diproses oleh ESP32 dan dibandingkan dengan daftar UID yang telah didaftarkan. Apabila UID tidak terdaftar, proses autentikasi dihentikan dan solenoid lock tetap berada dalam kondisi terkunci.

Apabila UID terdaftar, sistem melanjutkan proses ke tahap kedua, yaitu pengiriman dan validasi OTP melalui Telegram Bot. Sistem menghasilkan OTP dengan masa berlaku tertentu, kemudian mengirimkan kode tersebut kepada pengguna melalui Telegram. Pengguna memasukkan OTP melalui bot, lalu sistem membandingkan OTP yang diterima dengan OTP yang telah dihasilkan. Jika OTP sesuai dan masih berada dalam batas waktu berlaku, ESP32 mengaktifkan relay untuk membuka solenoid lock selama durasi yang telah ditentukan. Jika OTP tidak sesuai atau melewati batas waktu berlaku, relay tidak diaktifkan dan solenoid lock tetap terkunci.



Gambar 1. Arsitektur Sistem Smart Keyless 2FA Berbasis ESP32, RFID, dan Telegram Bot



Gambar 2. Diagram Alur Autentikasi RFID dan OTP Telegram

2.2. Perangkat dan Bahan Penelitian

Perangkat keras yang digunakan dalam penelitian ini meliputi ESP32, modul RFID RC522, kartu RFID, relay module, solenoid lock 12V, catu daya eksternal, dan kabel penghubung. ESP32 digunakan sebagai pusat kendali sistem karena memiliki konektivitas WiFi yang diperlukan untuk komunikasi dengan Telegram Bot. Modul RFID RC522 digunakan untuk membaca UID kartu RFID, sedangkan relay digunakan sebagai sakelar elektronik untuk mengendalikan solenoid lock.

Solenoid lock tidak dihubungkan langsung ke ESP32 karena membutuhkan tegangan dan arus yang lebih besar dibandingkan keluaran pin mikrokontroler. Oleh karena itu, solenoid lock dikendalikan melalui relay dan catu daya eksternal 12V. Rancangan ini bertujuan agar ESP32 hanya berfungsi sebagai pengendali sinyal, sedangkan beban aktuator ditangani oleh rangkaian daya terpisah.

Perangkat lunak yang digunakan meliputi program pada ESP32 dan bot Telegram. Program ESP32 digunakan untuk membaca UID kartu, memvalidasi UID, menghasilkan OTP, mengatur komunikasi dengan bot Telegram, memvalidasi OTP yang dimasukkan pengguna, serta mengendalikan relay. Bot Telegram dibuat melalui BotFather dan digunakan sebagai media komunikasi antara sistem dan pengguna dengan memanfaatkan Telegram Bot API [14].

2.3. Implementasi Sistem

Implementasi perangkat keras dilakukan dengan menghubungkan RFID RC522 ke ESP32 menggunakan komunikasi SPI. Relay dihubungkan ke salah satu pin digital ESP32 untuk mengatur kondisi aktif dan tidak aktif pada solenoid lock. Solenoid lock dikendalikan melalui relay dengan sumber daya eksternal 12V.

Pada sisi perangkat lunak, sistem diprogram untuk menjalankan autentikasi secara berurutan. Proses dimulai dari pembacaan UID kartu RFID. Jika UID sesuai dengan daftar kartu yang terdaftar, sistem membuat OTP dan mengirimkannya melalui Telegram Bot. Setelah pengguna mengirimkan OTP kembali melalui Telegram, sistem melakukan validasi terhadap kode tersebut. Relay hanya diaktifkan apabila UID RFID dan OTP memenuhi kondisi yang telah ditentukan.

Penggunaan OTP dibatasi oleh waktu berlaku tertentu agar kode tidak digunakan di luar sesi autentikasi. Namun, pengujian terhadap penyalahgunaan OTP, seperti penggunaan ulang OTP atau percobaan brute force, hanya dapat disimpulkan apabila skenario tersebut benar-benar diuji dalam penelitian.

2.4. Skenario Pengujian

Pengujian dilakukan untuk mengetahui kesesuaian respons sistem terhadap beberapa kondisi autentikasi. Skenario utama yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Kartu RFID terdaftar dan OTP valid.
2. Kartu RFID terdaftar dan OTP tidak valid.
3. Kartu RFID tidak terdaftar.

Pada skenario pertama, sistem diharapkan membuka solenoid lock karena kedua tahap autentikasi terpenuhi. Pada skenario kedua, sistem diharapkan menolak akses karena OTP tidak sesuai meskipun UID RFID terdaftar. Pada skenario ketiga, sistem diharapkan menolak akses sejak tahap pertama karena UID RFID tidak terdaftar.

Skenario tambahan dapat dilakukan untuk menguji OTP yang melewati batas waktu berlaku dan OTP yang digunakan kembali. Namun, apabila skenario tambahan tersebut tidak dilakukan, maka pembahasan hasil tidak boleh menyatakan bahwa sistem telah mampu mengatasi seluruh bentuk penyalahgunaan OTP.

2.5. Parameter Pengujian

Parameter yang diamati dalam penelitian ini meliputi status pembacaan UID RFID, status validasi UID, status pengiriman OTP, kesesuaian OTP, respons relay, kondisi solenoid lock, dan waktu respons sistem. Status pembacaan UID digunakan untuk mengetahui apakah kartu RFID dapat terbaca oleh modul RC522. Status validasi UID digunakan untuk mengetahui apakah kartu termasuk dalam daftar yang terdaftar pada sistem.

Status pengiriman OTP digunakan untuk memastikan bahwa OTP hanya dikirim ketika UID RFID terdaftar. Kesesuaian OTP digunakan untuk menentukan apakah kode yang dimasukkan pengguna sesuai dengan kode yang dihasilkan sistem. Respons relay dan kondisi solenoid lock digunakan untuk mengetahui apakah sistem membuka atau menolak akses sesuai dengan hasil autentikasi. Waktu respons digunakan untuk mengetahui durasi proses dari pembacaan RFID sampai solenoid lock terbuka pada skenario akses valid.

2.6. Teknik Analisis Data

Data hasil pengujian dianalisis secara deskriptif kuantitatif. Analisis dilakukan dengan membandingkan respons aktual sistem terhadap respons yang diharapkan pada setiap skenario pengujian. Jika respons aktual sesuai dengan respons yang diharapkan, maka percobaan tersebut dinyatakan berhasil. Jika respons aktual tidak sesuai dengan respons yang diharapkan, maka percobaan tersebut dinyatakan gagal.

$$TK = (PB / TP) \times 100\% \quad (1)$$

$$TG = (PG / TP) \times 100\% \quad (2)$$

$$\bar{T} = (\Sigma_{i=1}^{n} T_i) / n \quad (3)$$

Keterangan variabel:
TK = Tingkat Keberhasilan
TG = Tingkat Kegagalan
PB = Jumlah Percobaan Berhasil

PG = Jumlah Percobaan Gagal
TP = Jumlah Seluruh Percobaan
$\bar{T}$ = Rata-rata Waktu Respons
T_i = Waktu respons pada percobaan ke-i
n = Jumlah percobaan

Untuk skenario akses valid, keberhasilan dihitung berdasarkan kemampuan sistem membuka solenoid lock ketika UID RFID terdaftar dan OTP yang dimasukkan sesuai. Untuk skenario akses tidak valid, keberhasilan dihitung berdasarkan kemampuan sistem menolak akses ketika OTP salah atau UID RFID tidak terdaftar. Dengan demikian, analisis tidak hanya menilai keberhasilan sistem dalam membuka kunci, tetapi juga menilai kesesuaian sistem dalam menolak akses yang tidak memenuhi syarat autentikasi.

Hasil pengujian dan perhitungan dari setiap skenario disajikan pada bagian Hasil dan Pembahasan. Kesimpulan penelitian dibatasi pada skenario yang diuji agar tidak menghasilkan klaim yang melebihi data pengujian.

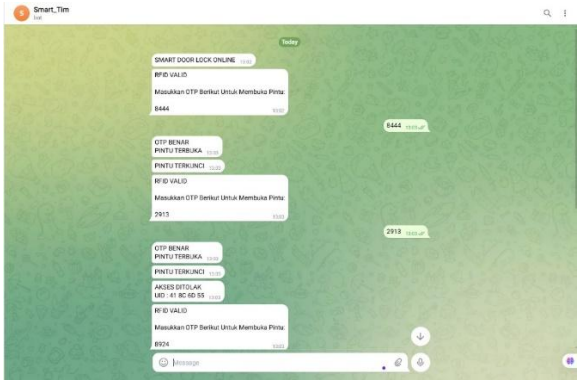
3. HASIL DAN PEMBAHASAN

3.1. Hasil Implementasi Sistem

Sistem smart keyless 2FA berbasis IoT telah diimplementasikan menggunakan ESP32, RFID RC522, Telegram Bot, relay, dan solenoid lock 12V. ESP32 berperan sebagai pusat kendali untuk membaca UID kartu RFID, memvalidasi data pengguna, mengirim dan memeriksa OTP melalui Telegram Bot, serta mengendalikan relay untuk membuka atau menutup solenoid lock.

Pada implementasi perangkat keras, RFID RC522 dihubungkan ke ESP32 melalui komunikasi SPI. Relay digunakan untuk mengendalikan solenoid lock 12V dengan sumber daya eksternal, sehingga solenoid tidak terhubung langsung ke pin ESP32. Pada implementasi perangkat lunak, sistem menjalankan autentikasi secara berurutan, yaitu membaca UID RFID, memeriksa status UID, mengirim OTP jika UID terdaftar, memvalidasi OTP yang dikirim pengguna, dan mengaktifkan relay apabila autentikasi sesuai dengan kondisi yang ditentukan.

Gambar 3. Prototipe Sistem Smart Keyless 2FA Berbasis ESP32, RFID RC522, Telegram Bot, Relay, dan Solenoid Lock



Gambar 4. Tampilan Pengiriman OTP melalui Telegram Bot

3.2. Hasil Pengujian Fungsional

Pengujian fungsional dilakukan untuk mengetahui kesesuaian respons sistem terhadap kombinasi UID RFID dan OTP. Sistem dinyatakan berhasil apabila respons aktual sesuai dengan respons yang diharapkan pada setiap skenario pengujian. Pengujian ini tidak digunakan untuk menyatakan bahwa sistem aman terhadap seluruh bentuk serangan, tetapi untuk menilai apakah alur autentikasi dua tahap berjalan sesuai rancangan.

Tabel 1. Hasil Pengujian Fungsional Autentikasi RFID dan OTP

No	Skenario Pengujian	UID	OTP	Respons Sistem	Jumlah Percobaan	Berhasil	Gagal	Keberhasilan
1	RFID terdaftar dan OTP valid	Terdaftar	Valid	Solenoid lock terbuka	10	10	0	100%
2	RFID terdaftar dan OTP tidak valid	Terdaftar	Tidak valid	Solenoid lock tetap terkunci	10	10	0	100%
3	RFID tidak terdaftar	Tidak terdaftar	OTP tidak dikirim	Solenoid lock tetap terkunci	10	10	0	100%

Berdasarkan Tabel 1, pengujian fungsional dilakukan pada tiga skenario autentikasi dengan masing-masing 10 kali percobaan. Pada skenario RFID terdaftar dan OTP valid, sistem berhasil membuka solenoid lock sebanyak 10 kali dari 10 percobaan, sehingga tingkat keberhasilan mencapai 100%. Pada skenario RFID terdaftar tetapi OTP tidak valid, sistem berhasil menolak akses dengan mempertahankan solenoid lock tetap terkunci sebanyak 10 kali dari 10 percobaan. Hasil serupa juga diperoleh pada skenario RFID tidak terdaftar, yaitu sistem tidak mengirimkan OTP dan solenoid lock tetap terkunci pada seluruh percobaan.

Secara keseluruhan, hasil pengujian menunjukkan bahwa sistem memberikan respons sesuai dengan rancangan pada seluruh skenario yang diuji. Akses hanya diberikan ketika UID RFID terdaftar dan OTP yang dimasukkan valid, sedangkan akses ditolak ketika OTP tidak valid atau UID RFID tidak terdaftar. Dengan demikian, logika autentikasi dua tahap pada prototipe ini berjalan sesuai skenario pengujian. Namun, hasil tersebut masih terbatas pada pengujian fungsional dan belum mencakup pengujian terhadap risiko keamanan lain, seperti duplikasi kartu RFID, percobaan OTP berulang, atau gangguan koneksi internet.

3.3. Hasil Pengujian Waktu Respons

Pengujian waktu respons dilakukan pada skenario kartu RFID terdaftar dan OTP valid. Pengujian ini bertujuan untuk mengetahui durasi proses autentikasi dari pembacaan RFID sampai solenoid lock terbuka. Waktu respons dapat dipengaruhi oleh koneksi WiFi, respons Telegram Bot, dan waktu pemrosesan pada ESP32.

Tabel 2. Hasil Pengujian Waktu Respons Sistem

No	Percobaan	Waktu Respons	Respons Sistem	Keterangan
1	Percobaan 1	0,3 detik	Solenoid lock terbuka	Berhasil
2	Percobaan 2	0,4 detik	Solenoid lock terbuka	Berhasil
3	Percobaan 3	0,1 detik	Solenoid lock terbuka	Berhasil
4	Percobaan 4	0,2 detik	Solenoid lock terbuka	Berhasil
5	Percobaan 5	0,3 detik	Solenoid lock terbuka	Berhasil
Rata-rata	-	0,26 detik	-	-

Berdasarkan Tabel 2, pengujian waktu respons dilakukan sebanyak lima kali pada skenario RFID terdaftar dan OTP valid. Hasil pengujian menunjukkan bahwa seluruh percobaan berhasil membuka solenoid lock, dengan waktu respons masing-masing sebesar 0,3 detik, 0,4 detik, 0,1 detik, 0,2 detik, dan 0,3 detik. Dari hasil tersebut, diperoleh rata-rata waktu respons sebesar 0,26 detik.

Nilai rata-rata tersebut menunjukkan waktu yang dibutuhkan sistem untuk memberikan respons setelah proses autentikasi dinyatakan valid hingga solenoid lock terbuka. Hasil ini menunjukkan bahwa sistem dapat mengaktifkan solenoid lock sesuai rancangan pada kondisi pengujian. Namun, nilai waktu respons tersebut tidak dapat digeneralisasi untuk seluruh kondisi penggunaan karena proses komunikasi dengan Telegram Bot tetap dipengaruhi oleh koneksi internet, respons layanan Telegram, dan kondisi jaringan saat pengujian dilakukan.

3.4.Pembahasan

Hasil pengujian menunjukkan bahwa sistem menerapkan autentikasi secara berlapis. Kartu RFID berfungsi sebagai tahap autentikasi pertama, sedangkan OTP Telegram berfungsi sebagai tahap autentikasi kedua. Akses hanya diberikan apabila kedua tahap tersebut memenuhi kondisi yang ditentukan. Dengan demikian, kepemilikan kartu RFID saja belum cukup untuk membuka solenoid lock apabila OTP yang dimasukkan tidak valid.

Pada skenario kartu RFID tidak terdaftar, sistem tidak mengirimkan OTP. Hal ini menunjukkan bahwa validasi UID dilakukan sebelum proses autentikasi kedua dijalankan. Mekanisme tersebut membuat sistem hanya memproses OTP untuk kartu yang telah didaftarkan. Namun, hasil ini masih terbatas pada pengujian fungsional dan belum mencakup pengujian terhadap risiko seperti duplikasi kartu RFID, percobaan OTP berulang, gangguan jaringan, atau kebocoran token Telegram Bot.

Jika dibandingkan dengan penelitian sebelumnya, sebagian sistem keamanan pintu berbasis IoT masih menempatkan RFID sebagai faktor utama autentikasi [5]–[9]. Pendekatan tersebut dapat membantu proses identifikasi pengguna, tetapi belum sepenuhnya mengurangi risiko apabila kartu RFID digunakan oleh pihak yang tidak berwenang. Penelitian yang menerapkan autentikasi berlapis, seperti kombinasi RFID e-KTP dan OTP melalui platform mobile, menunjukkan bahwa penambahan faktor autentikasi dapat memperkuat validasi akses [10]. Penelitian ini memiliki perbedaan pada penggunaan UID RFID sebagai tahap pertama dan OTP melalui bot Telegram sebagai tahap kedua pada prototipe berbasis ESP32. Oleh karena itu, kontribusi penelitian ini berada pada validasi alur autentikasi dua tahap serta pengujian kondisi akses diterima dan ditolak dalam sistem smart keyless berbasis IoT.

3.5. Keterbatasan Sistem

Penelitian ini masih memiliki beberapa keterbatasan. Pertama, proses OTP bergantung pada koneksi internet dan layanan Telegram Bot. Kedua, pengujian belum mencakup risiko duplikasi kartu RFID, brute force OTP, dan kebocoran token bot. Ketiga, sistem masih diuji dalam bentuk prototipe, sehingga hasilnya belum dapat langsung digeneralisasi untuk penggunaan operasional skala luas. Oleh karena itu, penelitian lanjutan dapat menambahkan pembatasan percobaan OTP, pencatatan log akses, pengujian kestabilan jaringan, serta pengujian keamanan yang lebih mendalam.

4. KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan prototipe sistem smart keyless 2FA berbasis IoT menggunakan ESP32, RFID RC522, Telegram Bot, relay, dan solenoid lock 12V. Sistem menerapkan autentikasi dua tahap, yaitu validasi UID RFID sebagai tahap pertama dan validasi OTP melalui Telegram Bot sebagai tahap kedua. Berdasarkan hasil pengujian fungsional pada tiga skenario utama, sistem memberikan respons sesuai dengan rancangan. Pada skenario RFID terdaftar dan OTP valid, sistem berhasil membuka solenoid lock sebanyak 10 kali dari 10 percobaan. Pada skenario RFID terdaftar tetapi OTP tidak valid, sistem berhasil menolak akses sebanyak 10 kali dari 10 percobaan. Pada skenario RFID tidak terdaftar, sistem juga berhasil menolak akses dengan tidak mengirimkan OTP dan mempertahankan solenoid lock tetap terkunci sebanyak 10 kali dari 10 percobaan.

Hasil pengujian waktu respons menunjukkan bahwa sistem memiliki rata-rata waktu respons sebesar 0,26 detik pada proses aktivasi solenoid lock setelah autentikasi dinyatakan valid. Hasil tersebut menunjukkan bahwa prototipe dapat menjalankan fungsi dasar autentikasi dua tahap sesuai skenario pengujian. Namun, penelitian ini masih terbatas pada pengujian fungsional dan belum mencakup pengujian keamanan lanjutan, seperti duplikasi kartu RFID, percobaan OTP berulang, kebocoran token Telegram Bot, maupun gangguan koneksi internet. Oleh karena itu, pengembangan selanjutnya dapat difokuskan pada penambahan pembatasan percobaan OTP, pencatatan log akses, pengujian kestabilan jaringan, serta penguatan mekanisme keamanan sistem sebelum diterapkan pada lingkungan operasional yang lebih luas.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada dosen pembimbing dan rekan sejawat yang telah memberikan bimbingan, masukan, dan saran selama proses penelitian. Terima kasih juga disampaikan kepada pihak yang telah membantu penyediaan sarana dan dukungan selama proses perancangan, implementasi, dan pengujian prototipe smart keyless 2FA.

DAFTAR PUSTAKA

[1] A. Kumar, A. K. Jain, and M. Dua, "A comprehensive taxonomy of security and privacy issues in RFID," *Complex Intell. Syst.*, vol. 7, no. 3, pp. 1327–1347, Jun. 2021, doi: 10.1007/s40747-021-00280-6.

[2] V. Kumar, R. Kumar, A. A. Khan, V. Kumar, Y.-C. Chen, and C.-C. Chang, "RAFI: Robust Authentication Framework for IoT-Based RFID Infrastructure," *Sensors*, vol. 22, no. 9, p. 3110, Apr. 2022, doi: 10.3390/s22093110.

[3] T.-M. Hoang, V.-H. Bui, and N.-H. Nguyen, "An Integrated Two-Factor Authentication Scheme for Smart Communications and Control Systems," *MENDEL*, vol. 29, no. 2, pp. 181–190, Dec. 2023, doi: 10.13164/mendel.2023.2.181.

[4] M. S. Ahmed, P. Kumar, and R. Singh, "Secure and Smart Door Lock with Dual-Factor Authentication for Critical Zones," *Math. Stat. Eng. Appl.*, vol. 72, no. 1, pp. 1491–1501, 2023, doi: 10.17762/msea.v72i1.2373.

[5] A. S. Permana, J. Arthady Sormin, and N. Ketut H.D, "Perancangan Sistem Keamanan Ruang Server Akses Doorlock Dengan Teknologi RFID Berbasis IoT Pada Ruang Server FISIP UNJANI," *Epsil. J. Electr. Eng. Inf. Technol.*, vol. 20, no. 2, pp. 100–110, Dec. 2022, doi: 10.55893/epsilon.v20i2.91.

[6] Azhar Jauharul Umam, D. Setiana, and A. Pradana, "Rancangan radio frequency identification (rfid) smart door lock system berbasis internet of things untuk manajemen membership fitness center," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 4, no. 2, pp. 359–365, Aug. 2023, doi: 10.37859/coscitech.v4i2.5126.

[7] A. N. M. Andreas and R. Arijanto, "Rancang Bangun Smart Home IoT dengan Integrasi Kunci Rfid dan Otomasi Elektronik," *bit-Tech*, vol. 7, no. 2, pp. 235–243, Dec. 2024, doi: 10.32877/bt.v7i2.1729.

[8] M. Wahyu Salfian, "Design of Door Security System using Rfid Based on IoT at Stmik Kaputama," *J. Artif. Intell. Eng. Appl.*, vol. 5, no. 1, pp. 604–610, Oct. 2025, doi: 10.59934/jaiea.v5i1.1367.

[9] Haris Asysyauqi, Moh. Ferdi Andriansyah, Lya Nurul Ulla, and Adi Sucipto, "Sistem Keamanan Pintu Otomatis Berbasis IoT dengan Teknologi RFID dan Aplikasi Mobile Menggunakan Metode Fuzzy Mamdani," *Modem J. Inform. dan Sains Teknol.*, vol. 3, no. 2, pp. 42–50, Apr. 2025, doi: 10.62951/modem.v3i2.405.

[10] U. Handasah, R. Afdila, A. Sani, R. Hendrawan, and M. Hamid, "Development of a Two-Layer Secure IoT Locker System Using e-KTP RFID and Mobile OTP via Blynk Platform," *J. Technomaterial Phys.*, vol. 7, no. 2, Oct. 2025, doi: 10.32734/jotp.v7i2.22170.

[11] A. Febriansyah and A. Yunanda, "SIMULASI SISTEM KEAMANAN DAN KENDALI GERBANG OTOMATIS PADA PORTAL PERUMAHAN MENGGUNAKAN TEKNOLOGI TANPA KUNCI BERBASIS IOT," *J. Comput. Sci. Inf. Technol.*, vol. 2, no. 3, pp. 324–337, Jun. 2025, doi: 10.70248/jcsit.v2i3.2088.

[12] M. W. Aryadi, I. K. R. Arthana, and P. H. Suputra, "SMART LOCK SYSTEM BERBASIS IOT MENGGUNAKAN ESP32 UNTUK KEAMANAN AKSES PUSAT DATA (STUDI KASUS: UPA TIK UNDIKSHA)," *J. Inform. dan Tek. Elektro Terap.*, vol. 14, no. 1, Jan. 2026, doi: 10.23960/jitet.v14i1.8826.

[13] Muarif, Ade Sumaedi, and Mardiansyah, "Monitoring Suhu Ruangan Server Jaringan Hostpot Berbasis Mikrokontroler NodeMCU ESP8266 Dengan Thingspeak," *J. Inf. Comput.*, vol. 2, no. 1, pp. 17–27, Jan. 2024, doi: 10.32493/jicomisc.v2i1.38638.

[14] Rajin Nahampun, Sewaka, and Taswanda Taryo, "Rancang Bangun Smartlock Detection Berbasis Mikrokotroller Dan ESP8266 Sebagai Bahan Media Pembelajaran Laboratorium Teknik Informatika Dan Komputer," *J. Inf. Comput.*, vol. 3, no. 1, pp. 74–83, Jan. 2025, doi: 10.32493/jicomisc.v3i1.40778.

Jicom : Journal Information & Computer
Volume 4, Nomor 2, Juli 2026, hlm.118-125
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Analisis Privasi Data Pengguna Shopee Berdasarkan Framework ISO 31000:2018

Siti Safira Tawetubun[*1], Satriani[2]
[1,2] Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia
Email: [*1]13020230217@student.umi.ac.id, [2]13020230073@student.umi.ac.id

(Naskah masuk: *11 Juni 2026*, diterima untuk diterbitkan: *31 Juli 2026*)

Abstrak: *Perkembangan e-commerce di Indonesia telah meningkatkan risiko kebocoran dan penyalahgunaan data pribadi pengguna. Penelitian ini penting karena belum ada studi yang secara spesifik menganalisis privasi data Shopee menggunakan kerangka kerja standar internasional. Penelitian ini bertujuan mengidentifikasi, menganalisis, mengevaluasi, dan memberikan rekomendasi perlakuan terhadap risiko privasi data pengguna Shopee menggunakan framework ISO 31000:2018. Metode penelitian menggunakan pendekatan kualitatif dengan studi literatur terhadap kebijakan privasi Shopee, regulasi Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022, jurnal ilmiah terindeks, dan berita online terkait kasus kebocoran data. Hasil penelitian mengidentifikasi 8 risiko utama (R1-R8) yang meliputi kebocoran data, pencurian akun, penyalahgunaan akses karyawan, pelanggaran UU PDP, serangan ransomware, pembobolan sistem pembayaran, kehilangan data akibat server crash, dan penjualan data ke pihak ketiga. Seluruh risiko berada pada level menengah dengan skor antara 5 hingga 12 berdasarkan perhitungan frekuensi dikalikan dampak. Rekomendasi mitigasi mencakup penerapan enkripsi end-to-end, two-factor authentication wajib, pembentukan tim kepatuhan UU PDP, serta implementasi disaster recovery plan. Penelitian ini berkontribusi sebagai studi pertama yang menggabungkan ISO 31000 dengan objek Shopee dan fokus pada privasi data pengguna.*

Kata Kunci *– E-commerce; ISO 31000; Privasi Data; Shopee*

Abstract: *The development of e-commerce in Indonesia has increased the risk of personal data leakage and misuse. This research is important because no study has specifically analyzed Shopee's data privacy using an international standard framework. This study aims to identify, analyze, evaluate, and provide risk treatment recommendations for Shopee user data privacy using the ISO 31000:2018 framework. The research method uses a qualitative approach with literature study of Shopee's privacy policy, PDP Law No. 27 of 2022, indexed scientific journals, and online news related to data breach cases. The results identified 8 main risks (R1-R8) including data leakage, account theft, employee access misuse, PDP law violations, ransomware attacks, payment system breaches, data loss due to server crashes, and sale of data to third parties. All risks are at the medium level with scores between 5 and 12 based on frequency multiplied by impact calculation. Mitigation recommendations include end-to-end encryption, mandatory two-factor authentication, formation of a PDP law compliance team, and disaster recovery plan implementation. This research contributes as the first study to combine ISO 31000 with Shopee as the object and focus on user data privacy.*

Keywords – *Data Privacy; E-commerce ; ISO 31000; Shopee*

1. PENDAHULUAN

Shopee merupakan platform e-commerce terbesar di Asia Tenggara yang didirikan pada tahun 2015. Perusahaan ini memiliki lebih dari 100 juta pengguna aktif bulanan di Asia Tenggara, dengan kontribusi terbesar berasal dari Indonesia. Shopee menyediakan berbagai layanan digital seperti belanja online, ShopeePay, ShopeeFood, ShopeeLive, serta ShopeeMall. Dalam setiap transaksi yang dilakukan, Shopee secara otomatis mengumpulkan data pribadi pengguna seperti nama lengkap, alamat email, nomor telepon, alamat pengiriman, riwayat transaksi, data lokasi, serta data pembayaran seperti kartu kredit atau e-wallet [1]. Pengumpulan data pribadi dalam skala besar membawa konsekuensi terhadap risiko keamanan data. Pada tahun 2020, data sekitar 15 juta akun pengguna Shopee diduga bocor dan diperjualbelikan di forum online [1]. Peningkatan kasus penipuan mengatasnamakan Shopee dengan modus phishing juga menunjukkan lemahnya kesadaran pengguna terhadap keamanan data [2]. Risiko tidak hanya datang dari eksternal tetapi juga dari internal, seperti penyalahgunaan hak akses oleh karyawan [3].

Kebijakan privasi Shopee mengatur bagaimana data pengguna dikumpulkan, digunakan, dan dilindungi [3]. Di Indonesia, perlindungan data pribadi secara resmi diatur dalam Undang-Undang Nomor 27 Tahun 2022

tentang Perlindungan Data Pribadi (UU PDP) [4]. Regulasi ini mewajibkan perusahaan e-commerce untuk melindungi data pengguna dan memberikan sanksi administratif maupun pidana bagi pelanggar. Sanksi yang diberikan sangat berat, berupa denda hingga 2% dari pendapatan tahunan dan pidana penjara maksimal 4 hingga 6 tahun [5]. Privasi data adalah hak individu untuk mengontrol bagaimana data pribadi mereka dikumpulkan, digunakan, dan disimpan oleh pihak lain [6]. Risiko didefinisikan sebagai pengaruh ketidakpastian terhadap pencapaian tujuan organisasi [7]. Manajemen risiko adalah proses sistematis untuk mengidentifikasi, menganalisis, mengevaluasi, menangani, dan memantau risiko secara berkelanjutan [7]. ISO 31000:2018 adalah standar internasional untuk manajemen risiko yang bersifat generik dan dapat diterapkan oleh berbagai organisasi [7]. Pengelolaan data dalam skala besar merupakan tantangan tersendiri di era digital. Yakin [8] menerapkan metode Content Based Image Retrieval (CBIR) pada sistem pencarian gambar digital, yang mengilustrasikan kompleksitas pengelolaan data multimedia. Pendekatan tersebut memberikan wawasan relevan bagi pengelolaan data pribadi pada platform e-commerce. Prinsip-prinsip dalam pengelolaan data digital ini relevan dengan konteks pengelolaan data pribadi pengguna e-commerce.

Berbagai penelitian sebelumnya telah membahas keamanan data Shopee. Terdapat beberapa keterbatasan penelitian yang menganalisis keamanan data pribadi pengguna Shopee dengan pendekatan deskriptif kualitatif, tetapi tidak menggunakan framework manajemen risiko yang baku [1]. Penelitian meninjau sistem keamanan data Shopee secara umum, tanpa melakukan identifikasi dan analisis risiko secara sistematis [2]. Penelitian membahas tanggung jawab hukum Shopee dalam kasus penyalahgunaan data, namun masih terbatas pada aspek yuridis, bukan manajemen risiko operasional [3]. Penelitian membahas perlindungan hukum data konsumen Shopee dari perspektif hukum, tanpa pendekatan manajemen risiko [6]. Mengidentifikasi berbagai tantangan dan perspektif dalam manajemen risiko pribadi serta privasi data di konteks Indonesia [9]. Beberapa penelitian telah menerapkan ISO 31000 pada e-commerce secara umum [10], [11], [12] belum ada penelitian yang secara spesifik menggabungkan framework ISO 31000 dengan objek Shopee dan fokus pada privasi data pengguna. Menganalisis manajemen risiko TI menggunakan COBIT 2019 dan ISO 31000 pada industri Jumputan, yang menunjukkan bahwa pendekatan terintegrasi dapat diterapkan di berbagai sektor industri termasuk e-commerce yang dilakukan oleh Sutabri [13]. Penelitian tentang efektivitas platform e-commerce dalam mendukung bisnis juga telah dilakukan oleh Muhammad [14], namun fokusnya pada aspek bisnis dan pemasaran, bukan pada privasi data pengguna.

Penelitian ini bertujuan mengidentifikasi risiko-risiko privasi data pengguna Shopee, menganalisis tingkat frekuensi dan dampak dari setiap risiko, mengevaluasi level risiko untuk menentukan prioritas penanganan, dan memberikan usulan perlakuan risiko berdasarkan ISO 31000:2018. Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan manajemen risiko privasi data pada platform e-commerce, khususnya Shopee, serta menjadi referensi bagi penelitian selanjutnya di bidang keamanan data dan perlindungan privasi pengguna.

2. METODE PENELITIAN

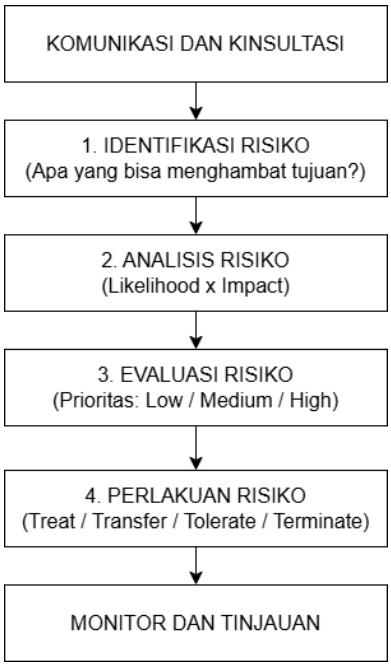
Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur (library research). Metode ini dipilih sejalan dengan tujuan penelitian untuk mengidentifikasi, menganalisis, mengevaluasi, dan memberikan rekomendasi perlakuan risiko privasi data pengguna Shopee berdasarkan kajian terhadap berbagai sumber pustaka yang relevan [7], [10], [11].

2.1. Jenis dan Sumber Data

Penelitian ini menggunakan data sekunder yang diperoleh dari tiga kategori sumber. Pertama, dokumen resmi kebijakan privasi Shopee [4]. Kedua, Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022 [4]. Pendekatan manajemen risiko juga telah dikembangkan oleh National Institute of Standards and Technology (NIST) melalui NIST SP 800-30 yang berfokus pada risiko sistem teknologi informasi [15]. Ketiga, jurnal ilmiah nasional dan internasional terindeks serta media massa berita online terkait kasus kebocoran data Shopee [1], [6], [10].

2.2. Tahapan Penelitian

Penelitian ini mengacu pada siklus manajemen risiko ISO 31000:2018 yang terdiri dari empat tahapan utama, yaitu identifikasi risiko, analisis risiko, evaluasi risiko, dan perlakuan risiko [7], [16]. Gambar 1 menunjukkan tahapan penelitian yang dilakukan.



Gambar 1. Tahapan Penelitian

2.3. Skala Penilaian Risiko

Penilaian frekuensi dan dampak menggunakan skala 1 sampai 5 yang mengacu pada tingkat kemungkinan terjadinya risiko dan tingkat keparahan dampak yang ditimbulkan [10]. Tabel 1 dan Tabel 2 masing-masing menunjukkan skala penilaian frekuensi dan dampak yang digunakan dalam penelitian ini.

Tabel 1. Skala Penilaian Frekuensi

Nilai	Kategori	Keterangan
1	Sangat Kecil	Tidak pernah terjadi > 5 tahun
2	Kecil	Jarang terjadi 3-5 tahun
3	Sedang	Terkadang terjadi 2-4 tahun
4	Berat	Sering terjadi 1-2 tahun
5	Sangat Berat	Pasti terjadi < 1 tahun

Tabel 2. Skala Penilaian Dampak

Nilai	Keterangan
1	Tidak mengganggu aktivitas proses bisnis
2	Sedikit menghambat proses bisnis
3	Mengganggu proses bisnis
4	Menghambat bagian tertentu proses bisnis
5	Menghambat serta mengganggu seluruh proses bisnis

3. HASIL DAN PEMBAHASAN

3.1. Identifikasi Risiko

Berdasarkan kajian terhadap kebijakan privasi Shopee [3], literatur kasus kebocoran data [1], [2], [12], dan regulasi UU PDP [4], ditemukan 8 risiko utama privasi data pengguna Shopee. Tabel 3 menyajikan hasil identifikasi risiko lengkap dengan kode, nama risiko, dan sumber risikonya.

Tabel 3. Identifikasi Risiko Privasi Data Pengguna Shopee

Kode	Kategori	Keterangan

R1	Kebocoran data pribadi pengguna	Peretasan server [1], [2]
R2	Pencurian akun pengguna	Phishing / Social engineering [3]
R3	Penyalahgunaan hak akses karyawan	Human error / Insider threat [17]
R4	Pelanggaran terhadap UU PDP	Ketidakpatuhan regulasi [4], [5], [6]
R5	Serangan ransomware	Malware [11], [18]
R6	Pembobolan sistem pembayaran	Hacker [2]
R7	Kehilangan data akibat server crash	Gangguan teknis [10]
R8	Penjualan data ke pihak ketiga	Kebijakan internal [3], [6]

Berdasarkan Tabel 3, terdapat 8 risiko utama yang dikelompokkan ke dalam lima kategori, yaitu ancaman eksternal (R1, R2, R5, R6), ancaman internal (R3), regulasi (R4), kegagalan sistem (R7), dan kebijakan (R8).

3.2. Analisis Risiko

Analisis risiko dilakukan dengan memberikan nilai frekuensi dan dampak pada setiap risiko yang telah diidentifikasi. Nilai frekuensi dan dampak ditentukan berdasarkan kajian literatur dan kasus-kasus yang pernah terjadi pada platform e-commerce [3], [17]. Tabel 4 menyajikan hasil analisis frekuensi dan dampak untuk kedelapan risiko tersebut.

Tabel 4. Hasil Analisis Frekuensi dan Dampak Risiko Privasi Data Shopee

Kode	Nama Risiko	Frekuensi	Dampak
R1	Kebocoran data pribadi pengguna	2	5
R2	Pencurian akun pengguna	3	4
R3	Penyalahgunaan hak akses karyawan	2	4
R4	Pelanggaran terhadap UU PDP	2	5
R5	Serangan ransomware	2	5
R6	Pembobolan sistem pembayaran	1	5
R7	Kehilangan data akibat server crash	3	4
R8	Penjualan data ke pihak ketiga	1	5

Berdasarkan Tabel 4, nilai frekuensi tertinggi (nilai 3) terdapat pada risiko pencurian akun pengguna (R2) dan kehilangan data akibat server crash (R7). Nilai dampak tertinggi (nilai 5) terdapat pada hampir semua risiko kecuali R2 dan R7 (nilai 4). Hal ini mengindikasikan bahwa sebagian besar risiko privasi data memiliki konsekuensi yang sangat serius terhadap kelangsungan bisnis Shopee.

3.3. Evaluasi Risiko

Evaluasi risiko bertujuan untuk menentukan level prioritas dari setiap risiko berdasarkan kombinasi nilai frekuensi dan dampak. Tingkat risiko ditentukan dengan rumus:

$$Risk\ Score = Frequency \times Impact \quad (1)$$

Kemudian diklasifikasikan ke dalam kategori Rendah (1-4), Menengah (5-12), atau Tinggi (13-25). Tabel 5 menyajikan hasil evaluasi level risiko untuk setiap kode risiko.

Tabel 5. Level Risiko Privasi Data Pengguna Shopee

Kode	Frekuensi	Dampak	Skor Risiko	Level
R1	2	5	10	Menengah
R2	3	4	12	Menengah
R3	2	4	8	Menengah
R4	2	5	10	Menengah
R5	2	5	10	Menengah
R6	1	5	5	Menengah
R7	3	4	12	Menengah

R8	1	5	5	Menengah

Berdasarkan Tabel 5, seluruh risiko privasi data pengguna Shopee berada pada level Menengah dengan nilai tingkat risiko antara 5 hingga 12. Tidak ada risiko yang masuk kategori Tinggi (13-25) maupun Rendah (1-4). Hal ini menunjukkan bahwa semua risiko tersebut memerlukan tindakan pengendalian yang sistematis dan berkelanjutan.

Temuan ini sejalan dengan penelitian yang menganalisis strategi keamanan digital Tokopedia menggunakan ISO 27001 dan ISO 31000, yang juga menemukan bahwa risiko keamanan data pada platform e-commerce umumnya berada pada level menengah [18]. Analisis risiko keamanan informasi menggunakan ISO 31000:2018 dan ISO 27001:2022 menemukan bahwa pendekatan terintegrasi efektif untuk mengidentifikasi dan mengevaluasi risiko di lingkungan digital [16]. Konferensi ACM International Conference menegaskan bahwa analisis risiko TI berbasis ISO 31000 memberikan kerangka kerja yang komprehensif untuk mengidentifikasi dan mengelola risiko keamanan informasi [19].

3.4. Perlakuan Risiko

Perlakuan risiko merupakan tahap akhir dari penilaian risiko yang bertujuan untuk memberikan usulan tindakan dalam menangani setiap risiko yang telah diidentifikasi. Strategi perlakuan risiko yang dapat dipilih meliputi: Accept (menerima risiko), Avoid (menghindari risiko), Transfer (mengalihkan risiko), dan Mitigate (mengurangi risiko) [7], [10], [11]. Tabel 6 menyajikan usulan perlakuan risiko untuk setiap kode risiko.

Tabel 6. Usulan Perlakuan Risiko Privasi Data Shopee

Kode	Level	Usulan Perlakuan Risiko	Rekomendasi
R1	Menengah	Enkripsi end-to-end, penetration testing rutin, update security patch [12], [20]	Mitigate
R2	Menengah	2FA wajib, edukasi phishing, deteksi login mencurigakan [2]	Mitigate
R3	Menengah	Least privilege access, logging akses, pelatihan keamanan [17]	Mitigate
R4	Menengah	Bentuk tim kepatuhan, audit berkala, konsultasi ahli hukum [4], [5]	Mitigate
R5	Menengah	Backup 3-2-1, antivirus, restore drill berkala [11], [18]	Mitigate
R6	Menengah	Tokenisasi, PCI DSS, enkripsi transaksi [2]	Mitigate
R7	Menengah	Disaster Recovery Plan, redundant server, backup harian [10]	Mitigate
R8	Menengah	Kebijakan internal, opsi opt-out, transparansi [3], [6]	Accept

Berdasarkan Tabel 6, terdapat 7 risiko yang direkomendasikan untuk Mitigate (mengurangi risiko melalui penerapan kontrol), dan 1 risiko yaitu penjualan data ke pihak ketiga (R8) direkomendasikan untuk Accept (diterima) dengan catatan Shopee harus transparan dan memberikan opsi kepada pengguna. Literature review mengidentifikasi bahwa strategi keamanan data yang efektif meliputi enkripsi, kontrol akses, dan kepatuhan regulasi [12]. Pentingnya perencanaan manajemen risiko yang terstruktur dalam bisnis e-commerce untuk mengantisipasi berbagai ancaman keamanan data juga telah ditekankan dalam penelitian sebelumnya [20].

3.5. Pembahasan Temuan

Analisis terhadap delapan risiko utama menunjukkan bahwa seluruh risiko berada pada tingkat menengah dengan skor antara 5 hingga 12. Kondisi ini mengindikasikan bahwa meskipun tidak terdapat risiko pada kategori tinggi, seluruh risiko tetap memerlukan pengendalian yang sistematis dan berkelanjutan.

3.5.1. Risiko dengan Dampak Sangat Besar (Skor Dampak 5)

Risiko R1 (kebocoran data pribadi) dengan skor 10 menempati perhatian utama karena dampaknya yang sangat berat (5), meskipun frekuensinya tergolong rendah (2). Kebocoran data umumnya disebabkan oleh celah keamanan server yang dieksploitasi oleh peretas eksternal. Dampak dari kebocoran data sangat luas, meliputi kerugian finansial bagi pengguna, hilangnya kepercayaan publik terhadap platform Shopee, serta

potensi sanksi hukum berdasarkan UU PDP yang dapat berupa denda hingga 2% dari pendapatan tahunan [1], [2], [4].

Risiko R4 (pelanggaran terhadap UU PDP) juga memiliki skor 10 dengan dampak 5. Pelanggaran terhadap regulasi perlindungan data pribadi dapat terjadi akibat ketidakpatuhan Shopee dalam mengelola data pengguna. Sanksi yang diberikan tidak hanya berupa denda administratif tetapi juga pidana penjara bagi pihak yang bertanggung jawab. Oleh karena itu, pembentukan tim kepatuhan khusus dan audit berkala menjadi langkah yang sangat direkomendasikan [4], [5].

Risiko R5 (serangan ransomware) dengan skor 10 juga memiliki dampak sangat berat. Serangan ransomware dapat melumpuhkan seluruh sistem Shopee, mengenkripsi data pengguna, dan meminta tebusan. Selain kerugian finansial, serangan ini dapat mengakibatkan hilangnya data pengguna secara permanen jika cadangan data tidak tersedia. Strategi backup 3-2-1 (3 salinan data, 2 media berbeda, 1 di luar lokasi) dan restore drill berkala menjadi keharusan [11], [18].

Risiko R6 (pembobolan sistem pembayaran) memiliki skor 5 dengan dampak 5. Meskipun frekuensinya sangat kecil (1), konsekuensinya paling serius karena menyangkut data keuangan pengguna seperti nomor kartu kredit dan informasi rekening bank. Implementasi tokenisasi, kepatuhan terhadap standar PCI DSS (Payment Card Industry Data Security Standard), serta enkripsi end-to-end untuk setiap transaksi menjadi strategi mitigasi yang wajib diterapkan [2].

Risiko R8 (penjualan data ke pihak ketiga) juga memiliki skor 5 dengan dampak 5. Risiko ini berkaitan dengan kebijakan internal Shopee yang memungkinkan data pengguna dibagikan kepada mitra bisnis atau pihak ketiga lainnya. Meskipun direkomendasikan untuk di-Accept (diterima), Shopee tetap wajib memberikan transparansi penuh kepada pengguna melalui kebijakan opt-out yang jelas dan mudah diakses [3], [6].

3.5.2. Risiko dengan Frekuensi Tertinggi (Skor Frekuensi 3)

Risiko R2 (pencurian akun pengguna) mencatat skor tertinggi (12) akibat frekuensi yang tergolong sedang (3) dan dampak 4. Teknik phishing dan social engineering menjadi faktor dominan dalam risiko ini. Pencurian akun biasanya terjadi karena pengguna tertipu oleh tautan palsu yang mengatasnamakan Shopee. Penerapan two-factor authentication (2FA) yang wajib bagi seluruh pengguna, edukasi berkala tentang modus phishing, serta sistem deteksi login mencurigakan menjadi strategi mitigasi yang paling efektif [2], [3].

Risiko R7 (kehilangan data akibat server crash) juga memiliki skor 12 dengan frekuensi 3 dan dampak 4. Gangguan teknis pada server dapat disebabkan oleh lonjakan trafik, kesalahan konfigurasi, atau kerusakan hardware. Kehilangan data akibat server crash dapat mengganggu operasional bisnis dan merugikan pengguna yang transaksinya tidak terekam. Implementasi Disaster Recovery Plan (DRP), penggunaan redundant server, serta backup data harian menjadi solusi utama untuk mengantisipasi risiko ini [10].

3.5.3. Risiko Internal

Risiko R3 (penyalahgunaan hak akses karyawan) memiliki skor 8 dengan dampak 4 dan frekuensi 2. Risiko ini bersifat internal dan sering kali tidak terdeteksi karena berasal dari karyawan yang memiliki akses sah ke sistem. Penyalahgunaan akses dapat berupa kebocoran data yang disengaja maupun ketidaksengajaan (human error). Penerapan prinsip least privilege (hak akses seminimal mungkin), logging dan monitoring akses secara berkala, serta pelatihan keamanan rutin bagi karyawan menjadi strategi mitigasi yang direkomendasikan [17].

3.5.4. Implikasi Manajerial

Secara keseluruhan, temuan ini mengindikasikan bahwa meskipun Shopee telah memiliki kebijakan privasi, implementasi teknis dan tata kelola risiko masih memerlukan peningkatan yang sistematis. Shopee perlu memprioritaskan penanganan risiko dengan dampak sangat berat (R1, R4, R5, R6, R8) meskipun frekuensinya rendah, karena konsekuensinya dapat mengancam kelangsungan bisnis. Di sisi lain, risiko dengan frekuensi tinggi (R2 dan R7) memerlukan perhatian pada aspek operasional dan edukasi pengguna.

Rekomendasi utama yang dapat diberikan kepada Shopee meliputi penerapan enkripsi end-to-end untuk seluruh data pengguna, kewajiban two-factor authentication bagi seluruh akun, pembentukan tim kepatuhan UU PDP yang bertugas melakukan audit berkala, implementasi Disaster Recovery Plan yang diuji secara rutin, serta peningkatan transparansi kebijakan privasi kepada pengguna.

4. KESIMPULAN

Berdasarkan hasil analisis privasi data pengguna Shopee menggunakan framework ISO 31000:2018, dapat ditarik kesimpulan sebagai berikut:

1. Identifikasi risiko menghasilkan 8 risiko utama privasi data pengguna Shopee, yaitu kebocoran data pribadi (R1), pencurian akun pengguna (R2), penyalahgunaan hak akses karyawan (R3), pelanggaran UU PDP (R4), serangan ransomware (R5), pembobolan sistem pembayaran (R6), kehilangan data akibat server crash (R7), dan penjualan data ke pihak ketiga (R8).
2. Analisis risiko menunjukkan bahwa nilai frekuensi tertinggi (nilai 3) terdapat pada risiko pencurian akun pengguna (R2) dan kehilangan data akibat server crash (R7), sedangkan nilai dampak tertinggi (nilai 5) terdapat pada hampir semua risiko kecuali R2 dan R7 (nilai 4).
3. Evaluasi risiko menunjukkan bahwa seluruh risiko berada pada level Menengah dengan nilai tingkat risiko antara 5 hingga 12. Tidak ada risiko yang masuk kategori Tinggi (13-25) maupun Rendah (1-4).
4. Perlakuan risiko menghasilkan rekomendasi mitigasi untuk 7 risiko (mitigate) dan 1 risiko (accept). Risiko penjualan data ke pihak ketiga (R8) direkomendasikan untuk diterima dengan syarat Shopee transparan kepada pengguna.
5. Penerapan ISO 31000:2018 terbukti efektif sebagai framework untuk mengidentifikasi, menganalisis, mengevaluasi, dan memberikan rekomendasi perlakuan risiko privasi data secara sistematis dan terstruktur.

Keterbatasan penelitian ini adalah penggunaan data sekunder tanpa verifikasi langsung ke pihak Shopee. Penelitian mendatang disarankan melakukan pendekatan kuantitatif melalui survei kepada pengguna Shopee serta studi komparatif dengan platform e-commerce lainnya seperti Tokopedia dan Lazada [16], [18].

DAFTAR PUSTAKA

[1] T. A. Cahyaaty, I. Wijaya, M. Dafin, and A. Dzky, "Analisis Keamanan Data Pribadi Pada Pengguna E-Commerce Shopee Terhadap Ancaman Data Pribadi," vol. 5, no. 2, pp. 133–144, 2024, doi: https://doi.org/10.31599/mdpf3g55.

[2] Y. N. Silalahi and M. I. P. Nasution, "Tinjauan Sistem Keamanan Data Pelanggan di E-Commerce: Studi Kasus Platform Shopee," *J. Sist. Informasi, Manaj. dan Teknol. Inf.*, vol. 3, no. 2, pp. 113–122, 2025, doi: 10.33020/jsimtek.v3i2.813.

[3] D. T. Sonda, "Tinjauan Yuridis Tanggung Jawab Penyelenggara E-Commerce dalam Penyalahgunaan Data Pribadi oleh Pihak Ketiga dalam Transaksi Shopee Pay Later," Universitas Sumatera Utara, 2024.

[4] "UU No. 27 Tahun 2022." [Online]. Available: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

[5] R. Ayunda, "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?," *LAW REFORM*, vol. 18, no. 2, pp. 144–163, 2022, doi: 10.14710/lr.v18i2.43307.

[6] A. M. Chaniago, M. Siregar, and J. Arifiyanto, "Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi E-Commerce Shopee," *J. Sci. Soc. Res.*, vol. 8, no. 1, pp. 184–195, 2025.

[7] I. O. für Normung, *ISO 31000: 2018: Risk Management: Guidelines*. ISO, 2018.

[8] S. Yakin, T. Hasanuddin, and N. Kurniati, "Application of content based image retrieval in digital image search system," *Bull. Electr. Eng. Informatics*, vol. 10, no. 2, pp. 1122–1128, 2021, doi: 10.11591/EEI.V10I2.2713.

[9] A. Setiawan and R. Puspitadewi, "Challenges and Perspectives on Personal Risk Management and Data Privacy in the Indonesian Context," *Rev. Integr. Bus. Econ. Res.*, vol. 15, p. 3, 2026.

[10] Sulpawati, N. Choirunnisa, and H. F. Rohman, "Strategi Manajemen Risiko Operasional dalam Bisnis E-Commerce untuk Menghadapi Tantangan dan Menemukan Solusi," *J. Manaj. dan Pemasar. (Jump.)*, vol. 4, no. 1, 2025, doi: 10.51771/jumper.v4i1.1729.

[11] E. K. Usmany, "Information Security Planning with Risk Management Using ISO 31000:2018 at E-Commerce XYZ," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 33, pp. 75–89, 2025, doi: 10.52783/jisem.v10i33s.5460.

[12] A. P. Kehista *et al.*, "Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review)," *J. Ilmu Manaj. Terap.*, vol. 4, no. 5, pp. 625–632, 2023, doi: 10.31933/JIMT.V4I5.1541.

[13] T. Sutabri, Y. Pratama, M. I. Herdiansyah, and W. Cholil, "Information Technology Risk Management Analysis Using COBIT and ISO at Jumputan Industry," *Int. J. Informatics Vis.*, vol. 9, no. 6, pp. 2418–2429, 2025, doi: 10.62527/JOIV.9.6.3236.

[14] A. Muhammad, C. P. T.W, R. Fauzi, and Pramono, "Efektivitas Platform E-Commerce Dalam Mendukung Bisnis Kaos Anime," *J. Inf. \& Comput.*, vol. 3, no. 1, pp. 21–31, 2025, doi: 10.32493/JICOMISC.V3I1.46981.

[15] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems," 2002. doi: https://doi.org/10.6028/NIST.SP.800-30.

[16] A. Ulya, A. Karima, T. S. A. Sukiman, A. Zulfia, and R. Rahmawati, "Information Security Risk Analysis Using ISO 31000:2018 and ISO 27001:2022," *Brill. Res. Artif. Intell.*, vol. 5, no. 2, pp. 843–853, 2025, doi: 10.47709/brilliance.v5i2.6564.

[17] T. M. Muhtar and E. Radhiansyah, "Analisis Implementasi Kebijakan Perlindungan Data Pribadi dalam Perdagangan Digital di Indonesia Berdasarkan eTrade Readiness Assessment," *J. Integr. Int. Relations*, vol. 10, no. 2, pp. 157–179, 2025, doi: 10.15642/jiir.2025.10.2.157-179.

[18] M. M. R. Akbar, K. Yudhistiro, and A. R. Muslikh, "Analysis of Tokopedia Digital Security Strategy Against Cyber Threats Using the Risk Assessment Framework Approach," *J. Innov. Comput. Sci.*, vol. 4, no. 2, pp. 94–101, 2025, doi: 10.56347/JICS.V4I2.301.

[19] F. S. Lubis, V. S. Praditha, M. Lubis, M. F. Safitra, and Y. Z. Ramadhan, "IT Risk Analysis Based on Risk Management Using ISO 31000: Case study Registration Application at University XYZ," *Proc. 2023 9th Int. Conf. Ind. Bus. Eng.*, pp. 522–528, 2023, doi: 10.1145/3629378.3629464.

[20] M. Ekania, E. Hamdi, R. Indradewa, and F. Abadi, "Risk Management Planning in E-Commerce Companies PT. SIMPEL OM UNGGULAN "SIMPEL OMâ€□," *Syntax Idea*, vol. 5, no. 11, pp. 1939–1956, 2023, doi: 10.46799/SYNTAX-IDEA.V5I11.2661.

Jicom : Journal Information & Computer
Volume 04, Nomor 02, Juli 2026, hlm.126-137
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Rancang Bangun Sistem Pintu Otomatis Berbasis *Iot With Fingerprint And Vibration Sensors* untuk Keamanan Cerdas

Muhamad Alfi Nurohman*[1], Eneng Susilistia Agustini[2]
[1,2)]Program Studi Sistem Komputer, Universitas Pamulang Kampus Kota Serang
Email: [*1]alfinurhmn28@gmail.com, [2]dosen10009@unpam.ac.id

Abstrak: Penelitian ini dilatarbelakangi oleh keterbatasan sistem keamanan ruangan yang masih menggunakan kunci konvensional sehingga rentan terhadap pembobolan dan belum mendukung pemantauan jarak jauh. Penelitian ini bertujuan merancang dan membangun sistem keamanan pintu otomatis berbasis *Internet of Things (IoT)* untuk meningkatkan keamanan akses dan efektivitas pengawasan ruangan. Metode yang digunakan adalah penelitian eksperimental dengan pendekatan prototipe melalui tahapan analisis kebutuhan, perancangan sistem, implementasi perangkat keras dan perangkat lunak, serta pengujian menggunakan metode *Black Box Testing*. Sistem dikembangkan menggunakan mikrokontroler ESP32 yang terintegrasi dengan sensor sidik jari sebagai autentikasi akses, sensor getaran untuk mendeteksi upaya pembobolan, sensor PIR untuk mendeteksi gerakan, serta Bot Telegram sebagai media notifikasi dan kontrol jarak jauh. Hasil penelitian menunjukkan bahwa sistem mampu mengontrol akses pintu secara otomatis, mendeteksi aktivitas mencurigakan, serta mengirimkan notifikasi secara real-time kepada pengguna. Dengan demikian, sistem yang dirancang dapat meningkatkan keamanan ruangan dibandingkan sistem konvensional serta memberikan solusi keamanan yang lebih efektif, modern, dan responsif berbasis teknologi IoT.

Kata Kunci *– Internet of Things*, keamanan pintu, ESP32, *fingerprint*, telegram bot.

Abstract: *This research is motivated by the limitations of room security systems that still use conventional keys, making them vulnerable to burglary and not yet supporting remote monitoring. This research aims to design and build an Internet of Things (IoT)-based automatic door security system to improve access security and the effectiveness of room surveillance. The method used is experimental research with a prototype approach through the stages of needs analysis, system design, hardware and software implementation, and testing using the black box method. The system was developed using an ESP32 microcontroller integrated with a fingerprint sensor for access authentication, a vibration sensor to detect burglary attempts, a PIR sensor to detect motion, and a Telegram Bot as a notification and remote control medium. The results of the study show that the system is able to control door access automatically, detect suspicious activity, and send real-time notifications to users. Thus, the designed system can improve room security compared to conventional systems and provide a more effective, modern, and responsive security solution based on IoT technology*.

Keywords *– Internet of Things, security door, ESP32, fingerprint, telegram bot.*

1. PENDAHULUAN

Keamanan dalam ruangan adalah kebutuhan penting di berbagai sektor, termasuk rumah, laboratorium, kantor, dan *showroom.* Tingginya risiko pencurian dan akses tidak sah telah menyebabkan meningkatnya kebutuhan akan sistem keamanan modern. Sistem keamanan konvensional, yang masih menggunakan kunci manual, dianggap memiliki berbagai kelemahan, seperti mudah diduplikasi, rentan terhadap kehilangan kunci, dan kurang memiliki kemampuan pemantauan jarak jauh. Perkembangan teknologi *Internet of Things (IoT)* memberikan solusi baru untuk mengembangkan sistem keamanan berbasis otomatisasi dan pemantauan waktu nyata. *IoT* memungkinkan perangkat elektronik untuk saling terhubung melalui internet, memungkinkan mereka untuk bertukar data dengan cepat dan efisien [1]. Teknologi ini memungkinkan sistem keamanan untuk dipantau dan dikendalikan dari jarak jauh menggunakan smartphone atau perangkat lain yang terhubung ke internet.

Sistem keamanan berbasis autentikasi biometrik juga semakin banyak dikembangkan karena dianggap lebih aman daripada menggunakan kunci konvensional. Sidik jari adalah metode otentikasi yang efektif karena memanfaatkan karakteristik unik pengguna [2]. Penggunaan sistem keamanan berbasis sidik jari dan kata sandi dapat secara signifikan meningkatkan keamanan akses ruangan [3]. Selain itu, Integrasi ESP32 dan sensor sidik jari ke dalam kunci pintu pintar dapat meningkatkan efisiensi sistem keamanan berbasis *IoT* [4].

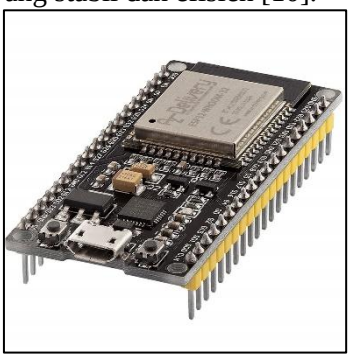
Selain autentikasi akses, sistem pemantauan dan notifikasi juga sangat penting dalam mengembangkan keamanan modern. sistem keamanan pintu berbasis ESP32 yang terintegrasi dengan Telegram sebagai alat pemantauan [5]. Efektivitas Telegram Bot sebagai alat pemantauan dan untuk mengirimkan notifikasi secara *real-time* [6]. Penggunaan notifikasi berbasis Telegram juga dianggap dapat meningkatkan respons pengguna terhadap ancaman keamanan [7]. Berdasarkan pengamatan di CV. Dua Sekawan Motor, sistem keamanannya masih menggunakan kunci manual dan tidak memiliki pemantauan keamanan berbasis internet. Situasi ini mengakibatkan pengawasan ruangan yang suboptimal dan meningkatkan risiko pencurian. Oleh karena itu, diperlukan sistem keamanan yang mampu mengontrol akses, memantau aktivitas, dan memberikan pemberitahuan *real-time* kepada pengguna.

1.1 *Internet Of Things (IoT)*

Internet of Things (IoT) adalah konsep komunikasi antara perangkat elektronik melalui internet, yang memungkinkan mereka untuk secara otomatis bertukar data. Teknologi *IoT* memungkinkan perangkat beroperasi secara real-time dan dikendalikan dari jarak jauh menggunakan internet. Dalam sistem keamanan, IoT memainkan peran penting dalam pemantauan, kontrol akses, dan mengirimkan notifikasi otomatis kepada pengguna. Penerapan IoT dalam sistem keamanan dalam ruangan dapat meningkatkan efektivitas pengawasan karena semua perangkat dapat diintegrasikan [1]. Selain itu, teknologi *IoT* memfasilitasi pemantauan keamanan rumah berbasis internet [8].

1.2 Mikrokontroler Esp32

ESP32 adalah mikrokontroler yang dikembangkan oleh *Espressif Systems* dan dilengkapi dengan Wi-Fi dan Bluetooth terintegrasi. ESP32 banyak digunakan dalam pengembangan sistem berbasis *IoT* karena kemampuan pemrosesan datanya yang kuat dan konsumsi daya yang rendah. Dalam penelitian ini, ESP32 digunakan sebagai pusat kontrol utama yang menghubungkan semua sensor dan aktuator dalam sistem keamanan pintu otomatis. Penggunaan ESP32 memungkinkan sistem untuk terhubung ke internet dan mengkomunikasikan data secara *real-time*. ESP32 sangat efektif untuk digunakan dalam sistem kunci pintu pintar berbasis *IoT* karena mendukung integrasi berbagai sensor dalam satu perangkat [9]. ESP32 memiliki kemampuan pemantauan berbasis *web* yang stabil dan efisien [10].



Gambar 2. Esp32

1.3 Sensor *Fingerprint* AS608

Pengenalan sidik jari adalah teknologi otentikasi biometrik yang memanfaatkan pola sidik jari manusia untuk mengidentifikasi pengguna secara unik. Sistem sidik jari menawarkan tingkat keamanan yang tinggi karena setiap individu memiliki pola sidik jari yang unik. Dalam penelitian ini, sensor sidik jari digunakan sebagai autentikasi utama untuk membuka pintu. Ketika sidik jari pengguna terdaftar terdeteksi, sistem secara otomatis membuka kunci solenoid pintu. Penggunaan sidik jari dalam sistem keamanan pintu dapat meningkatkan keamanan akses dibandingkan dengan kunci konvensional [2]. Selain itu, sensor sidik jari memiliki tingkat akurasi yang tinggi dalam identifikasi pengguna [11].

Gambar 3. Sensor *Fingerprint* AS608

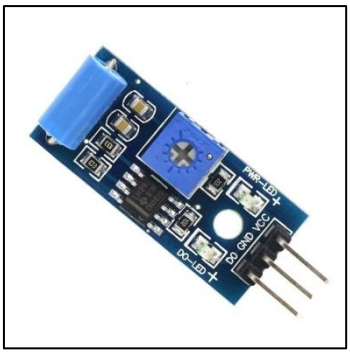
1.4 Sensor PIR HC-SR501

Sensor PIR adalah sensor yang digunakan untuk mendeteksi gerakan manusia berdasarkan radiasi inframerah tubuh. Sensor-sensor ini banyak digunakan dalam sistem keamanan dan sistem otomatisasi ruangan. Dalam penelitian ini, sensor PIR digunakan untuk mendeteksi aktivitas atau gerakan di sekitar ruangan. Ketika sensor mendeteksi gerakan, sistem mengaktifkan lampu indikator untuk memantau aktivitas. sensor PIR memiliki tingkat sensitivitas yang tinggi untuk mendukung sistem keamanan otomatis berbasis IoT [12]. integrasi sensor PIR dapat meningkatkan efektivitas pemantauan keamanan ruangan otomatis [13].

Gambar 4. Sensor PIR HC-SR501

1.5 Sensor Getaran SW-420

Sensor SW-420 adalah sensor getaran yang digunakan untuk mendeteksi getaran atau benturan pada objek tertentu. Sensor ini sering digunakan sebagai detektor pencurian dalam sistem keamanan. Dalam penelitian ini, sensor SW-420 digunakan untuk mendeteksi upaya pembobolan pintu. Ketika sensor mendeteksi getaran dengan intensitas tertentu, sistem mengaktifkan alarm *buzzer* dan mengirimkan notifikasi melalui Telegram Bot. Sensor getaran efektif sebagai sistem peringatan dini untuk aktivitas mencurigakan dalam sistem keamanan pintu [14]. Sensor SW-420 memiliki sensitivitas yang baik dalam mendeteksi getaran secara *real-time* [15].



Gambar 5. Sensor Getaran SW-420

1.6 Telegram Bot

Telegram Bot adalah layanan otomatis dalam aplikasi Telegram yang dapat digunakan untuk mengirim dan menerima pesan secara otomatis melalui internet. Telegram Bot banyak digunakan dalam sistem pemantauan berbasis *IoT* karena mudah diintegrasikan dengan mikrokontroler. Dalam penelitian ini, Bot Telegram digunakan sebagai alat pemantauan dan untuk mengirimkan notifikasi waktu nyata kepada pengguna ketika aktivitas mencurigakan atau upaya pencurian terjadi. Telegram Bot efektif sebagai alat pemantauan

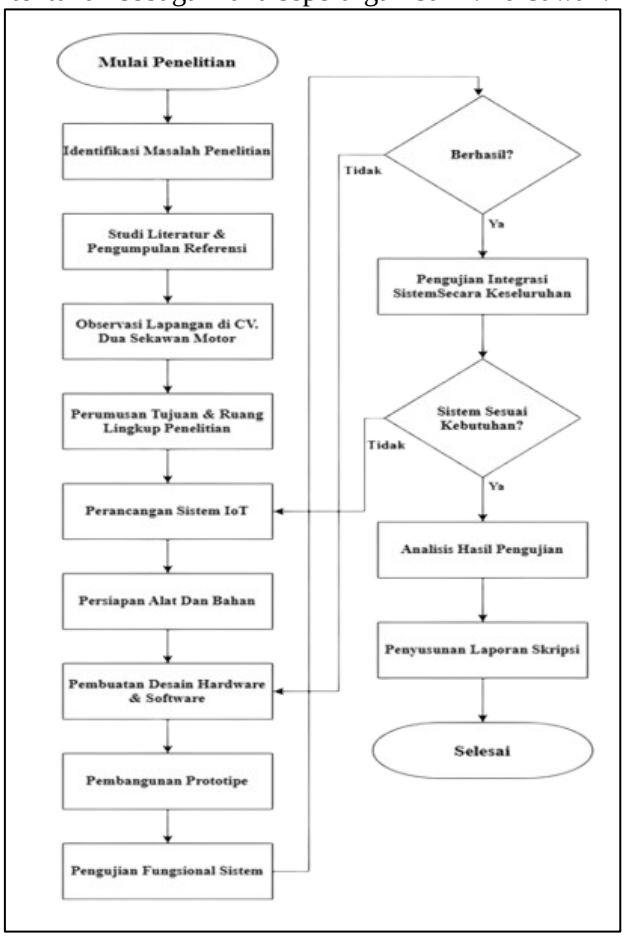
untuk sistem keamanan berbasis *IoT* karena responsnya cepat dan mudah digunakan [6]. Telegram dapat menjadi alat komunikasi yang efektif dalam sistem keamanan berbasis internet [7].

2. METODE PENELITIAN

Dalam penelitian ini, metode eksperimental yang dikombinasikan dengan pendekatan studi kasus diterapkan. Metode eksperimental dipilih karena penelitian ini memerlukan perancangan, implementasi, dan pengujian langsung dari prototipe sistem keamanan pintu otomatis berbasis *Internet of Things (IoT)*. Melalui fase eksperimental, para peneliti dapat mengevaluasi kinerja setiap komponen, seperti sensor sidik jari, sensor PIR, sensor getaran, buzzer, LED, LCD, dan mekanisme perintah melalui Telegram Bot. Di sisi lain, pendekatan studi kasus digunakan karena penelitian ini berfokus pada lokasi tertentu, yaitu sebuah ruangan tertentu di CV. Dua Sekawan Motor, yang menghadapi masalah keamanan tertentu. Pendekatan ini membantu para peneliti memahami situasi dengan lebih mendalam, mengidentifikasi kebutuhan sistem keamanan, dan menilai efektivitas prototipe yang dikembangkan ketika diterapkan dalam situasi dunia nyata.

2.1. Diagram Alur Penelitian

Diagram alur penelitian dibuat untuk memberikan representasi visual dari setiap tahap proses penelitian. Diagram ini bertujuan untuk memastikan bahwa semua langkah penelitian dapat dipahami secara sistematis dan struktural, mulai dari perumusan masalah dan pengumpulan referensi, desain sistem, implementasi perangkat keras dan perangkat lunak, hingga tahap pengujian dan evaluasi. Dengan diagram alur, hubungan antara tahap-tahap menjadi lebih jelas, memungkinkan alur kerja penelitian diikuti secara berurutan sesuai dengan rencana yang telah ditentukan sebagaimana seperti gambar 2.1 dibawah.

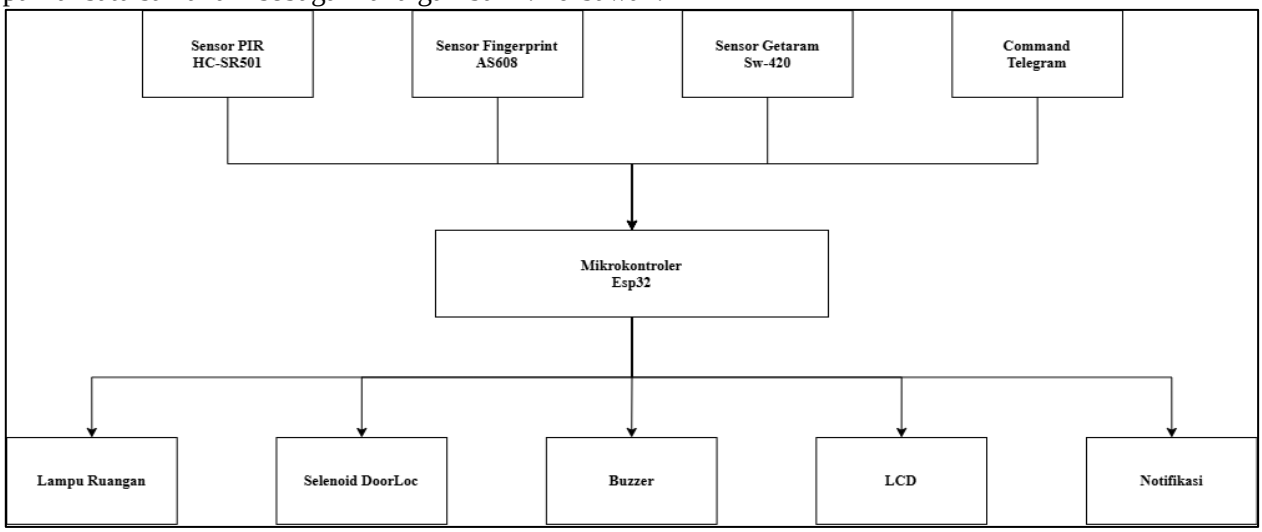


Gambar 6. Diagram Alur Penelitian

2.2. Diagram Blok Sistem

Pada tahapan ini melibatkan pembuatan gambaran sistem yang komprehensif, yang menggambarkan hubungan antara semua perangkat yang terlibat dalam desain sistem keamanan pintu otomatis berbasis *Internet of Things (IoT)*. Pada tahap ini, setiap komponen, seperti mikrokontroler ESP32, sensor sidik jari, dan chatbot Telegram sebagai media autentikasi akses utama, sensor PIR untuk mendeteksi keberadaan manusia, serta

sensor getaran sebagai indikator upaya pembobolan atau kerusakan pintu, dirancang untuk berinteraksi secara optimal satu sama lain sebagaimana gambar 2.2 dibawah.



Gambar 7. diagram Blok Sistem

2.3. Populasi Dan Sampel

Populasi dalam penelitian ini mencakup semua aktivitas akses pintu di ruang khusus di CV. Showroom Dua Sekawan Motor yang terletak di Desa Cigoong, Kecamatan Walantaka, Kota Serang, Banten. Sampel penelitian terdiri dari kegiatan pengujian akses pintu yang dilakukan menggunakan teknik pengambilan sampel yang digunakan adalah *purposive sampling*, di mana sampel dipilih berdasarkan skenario uji yang memenuhi persyaratan sistem. Dengan teknik pengumpulan data ini, diharapkan hasil penelitian dapat menggambarkan kinerja sistem keamanan pintu otomatis berbasis *Internet of Things (IoT)* yang telah dikembangkan dengan akurat, sebagaimana tabel 2.1 dibawah.

Tabel 1. Populasi Dan Sampel

Jenis Pengujian	Jumlah Sampel
Autentikasi Sidik Jari Valid	3x
Autentikasi Sidik Jari Tidak Valid	3x
Deteksi Pembobolan	3x
Deteksi Pergerakan PIR	3x

2.4. Teknik Pengujian Sistem

Pengujian dilakukan langsung pada prototipe sistem melalui beberapa skenario, menggunakan pengujian kotak hitam. Ini termasuk upaya akses pintu menggunakan autentikasi sidik jari, deteksi gerakan dalam ruangan, dan upaya pencurian yang disimulasikan menggunakan sensor getaran. Selain itu, keterlambatan antara deteksi sensor dan pemberitahuan kepada pengguna diukur untuk menilai kecepatan respons sistem. Dan dapat dilihat pada tabel 2.2 dibawah.

Tabel 2. Teknik Pengujian Sistem

No	Pengujian	Parameter	Kriteria	Hasil
1.	Autentikasi Fingerprint	Keberhasilan sidik jari	Selenoid terbuka dan LCD menampilkan "Pintu terbuka, Akses Diterima"	✓ / ✗
2.	Kegagalan Akses	Sidik Jari Tidak Terdaftar	Selenoid tetap dan LCD menampilkan "Pintu tertutup, Akses Ditolak"	✓ / ✗
3.	Notifikasi Telegram	Respon terhadap getaran	Notifikasi terkirim	✓ / ✗
4.	Sensor PIR	Deteksi pergerakan	LED menyala otomatis	✓ / ✗

5.	Alarm Keamanan	Getaran terdeteksi SW-420	Buzzer aktif dan notifikasi terkirim	✓ / ✗
6.	Perintah Chat Bot	Melakukan perintah: Open, Status, VibOn, VibOff, Enroll	Responsif output sistem ketika diberikan perintah dari chat bot telegram	✓ / ✗

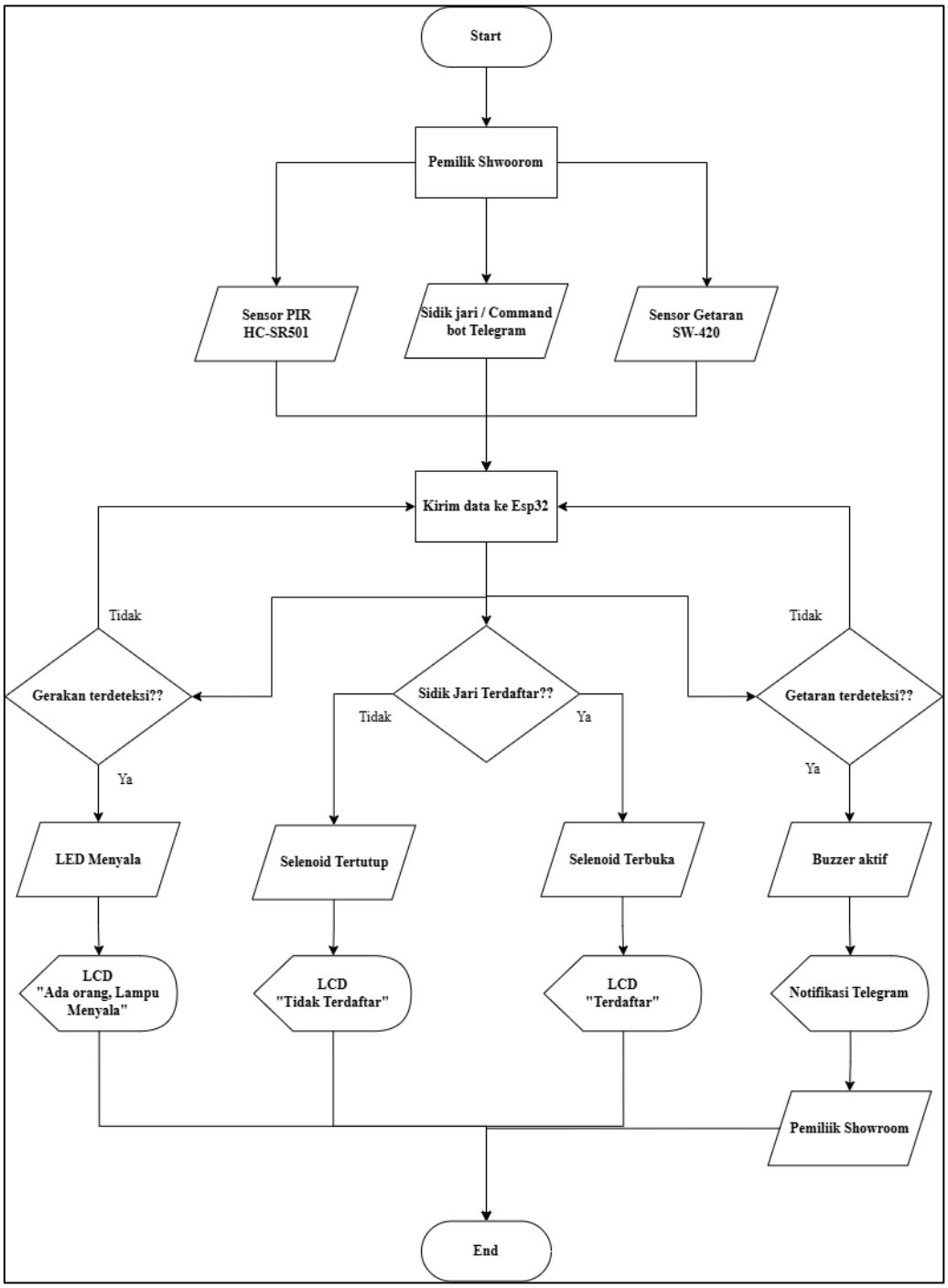
Dari tabel 2.2 diatas dengan serangkaian pengujian, sistem keamanan pintu otomatis berbasis *Internet of Things (IoT)* ini diharapkan dapat menunjukkan kinerja yang memenuhi persyaratan dan spesifikasi yang telah ditetapkan. Setiap tahap pengujian dilakukan untuk memastikan bahwa semua komponen, mulai dari sensor sidik jari, sensor PIR, sensor getaran, aktuator, hingga notifikasi melalui Telegram Bot, beroperasi secara optimal dan terintegrasi ke dalam satu sistem.

3. HASIL DAN PEMBAHASAN

Tahap ini menyajikan hasil dari proses desain untuk sistem keamanan pintu otomatis berbasis Internet of Things (IoT) yang dikembangkan dalam penelitian ini. Desain sistem terdiri dari dua komponen utama: desain perangkat keras dan desain perangkat lunak. Kedua komponen ini bekerja sama untuk menghasilkan sistem keamanan pintu yang beroperasi secara otomatis dan real-time.

3.1. Hasil *Flowchart* Arsitektur Sistem

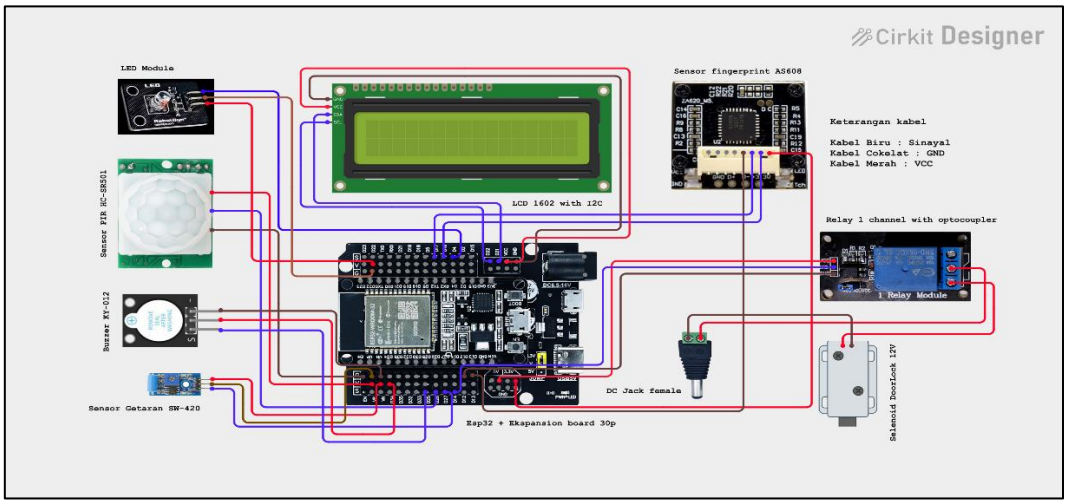
Konsep ini memungkinkan sistem berfungsi sebagai sistem keamanan fisik dan sistem pemantauan *Internet of Things (IoT)* jarak jauh. Diharapkan bahwa integrasi arsitektur secara keseluruhan akan meningkatkan keamanan, akuntabilitas, dan efektivitas pengawasan di ruangan-ruangan tertentu yang menerapkan konsep *One Gate System*. Seperti yang ditunjukkan pada gambar 3.1 dibawah.



Gambar 8. *Flowchart* Arsitektur Sistem

3.2. Hasil *Wiring* Sistem

Diagram pengkabelan keseluruhan bertujuan untuk menggabungkan semua komponen perangkat keras menjadi sistem yang kohesif dan saling terhubung. Pada titik ini, semua sensor dan aktuator yang digunakan, termasuk sensor sidik jari, sensor PIR, sensor getaran, buzzer, LED, LCD, dan modul komunikasi yang terhubung ke Telegram Bot, dirakit dan dihubungkan secara ringkas menggunakan mikrokontroler ESP32. Untuk memastikan bahwa distribusi daya dan aliran komunikasi data berjalan lancar dan memenuhi kebutuhan setiap komponen, pengkabelan dirancang secara sistematis. Dapat dilihat pada gambar 3.2 dibawah



Gambar 9. *Wiring* Sistem

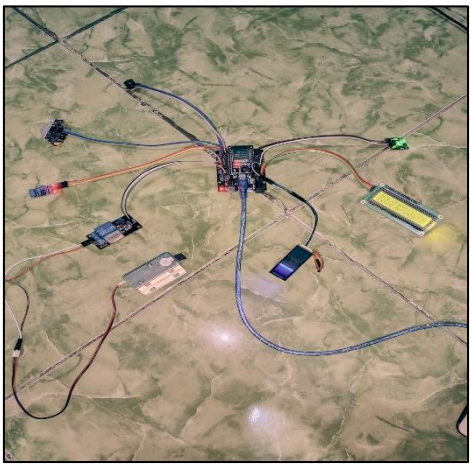
3.3. Hasil Desain Prototipe

Desain perangkat lunak adalah tahap konseptual dalam pengembangan sistem yang terjadi sebelum dan setelah proses pengkodean. Tahap ini bertujuan untuk menggambarkan struktur, alur kerja, dan interaksi antara modul perangkat lunak yang mengontrol sistem keamanan pintu otomatis berbasis *Internet of Things (IoT).* Desain perangkat lunak dikembangkan untuk memastikan proses implementasi program yang terfokus dan terstruktur yang memenuhi persyaratan sistem. Dilihat pada gambar 3.3 dibawah.

Gambar 10. Desain Prototipe

3.4. Hasil Integrasi Perangkat Keras

Integrasi ini dilakukan untuk memastikan bahwa setiap komponen dapat bekerja secara sinkron dan saling mendukung dalam melaksanakan fungsi sistem keamanan pintu otomatis berbasis *IoT*. Dengan integrasi yang tepat, sistem diharapkan dapat beroperasi secara stabil, responsif, dan sesuai dengan tujuan penelitian. Hasil integrasi perangkat keras dapat dilihat pada gambar 3.4 dibawah.



Gambar 11. Integrasi Perangkat Keras

3.5. Hasil Integrasi Prototipe Keseluruhan

Integrasi sistem secara keseluruhan dalam studi ini adalah langkah penting, yang menunjukkan bahwa semua komponen perangkat keras dan perangkat lunak bekerja sama untuk membentuk sistem keamanan pintu otomatis berbasis *Internet of Things (IoT)*. Integrasi ini mencakup koneksi antara sensor sidik jari, sensor PIR, sensor getaran, aktuator, mikrokontroler ESP32, dan platform telegram bot untuk notifikasi dan kontrol jarak jauh. Integrasi sistem secara keseluruhan dirancang menggunakan konsep sistem gerbang tunggal, di mana semua proses autentikasi, pemantauan, dan kontrol difokuskan pada satu titik akses. Pendekatan ini membuat sistem lebih efektif dalam memantau aktivitas masuk dan keluar sambil meminimalkan celah keamanan dari saluran lain. Dan dapat dilihat pada gambar 3.5 di halaman berikutnya.

Gambar 12. Integrasi Prototipe Keseluruhan

3.6. Hasil Pengujian

Pengujian sistem dalam penelitian ini dilakukan menggunakan metode *Black Box Testing*, yaitu metode pengujian yang berfokus pada fungsionalitas sistem berdasarkan kesesuaian antara input yang diberikan dan output yang dihasilkan, tanpa mempertimbangkan struktur internal program. Metode ini dipilih karena penelitian ini bertujuan untuk memastikan bahwa setiap fungsi dalam sistem keamanan pintu otomatis berbasis *Internet of Things (IoT)* beroperasi sesuai dengan spesifikasi yang telah dirancang pada tabel 3.1 dibawah.

Tabel 3. *Black Box Testing*

No	Skenario Uji	Input	Output Yang Diharapkan	Output Aktual	Hasil
1.	Sidik jari terdaftar	Sidik jari valid	Selenoin terbuka	Pintu terbuka	✓
2.	Sidik jari tidak terdaftar	Sidik jari tidak valid	Selenoid tetap tertutup	Pintu tertutup	✓
3.	Tidak ada getaran	Kondisi normal	Tidak ada alarm / notif	Tidak ada alarm, sistem idle	✓

4.	Ada getaran	Ada benturan	Buzzer aktif dan notif terkirim	Buzzer aktif dan notif terkirim	✓
5.	Ada pergerakan	Aktivitas manusia	Lampu LED menyala	Lampu LED menyala	✓
6.	Tidak Ada pergerakan	Tidak ada aktivitas	Lampu LED tidak menyala	Lampu LED tidak menyala	✓
7.	Notifikasi pembobolan	Deteksi getaran	Notif terkirim ke telegram	Pesan diterima	✓
8.	Perintah buka pintu	Perintah chat bot	Selenoid terbuka	Pintu terbuka	✓
9.	Perintah melihat status	Perintah chat bot	Tampilan status di telegram	Tampilan terkirim	✓
10.	Perintah vibon	Perintah chat bot	Sensor getaran aktif	Sensor getaran aktif	✓
11.	Perintah viboff	Perintah chat bot	Sensor getaran nonaktif	Sensor getaran nonaktif	✓

Hasil uji di atas menunjukkan bahwa integrasi ESP32 dengan Telegram Bot berfungsi dengan baik dan mendukung pemantauan dan pengendalian sistem jarak jauh.

3.7. Pembahasan

Berdasarkan hasil implementasi dan pengujian, sistem keamanan pintu otomatis berbasis *Internet of Things (IoT)* berhasil memenuhi tujuan penelitian. Integrasi sensor sidik jari, sensor getaran SW-420, sensor PIR, dan Telegram Bot secara signifikan meningkatkan efektivitas keamanan ruangan dibandingkan dengan sistem keamanan konvensional. Sistem sidik jari berhasil membatasi akses hanya untuk pengguna terdaftar, sehingga meminimalkan risiko akses tidak sah. Selain itu, sensor getaran SW-420 memberikan perlindungan tambahan dengan mendeteksi upaya pembobolan pintu melalui getaran tertentu. sensor getaran dapat digunakan sebagai sistem peringatan dini untuk aktivitas mencurigakan [14]. Penggunaan sensor PIR dalam penelitian ini memberikan fungsionalitas pemantauan tambahan dengan mendeteksi aktivitas atau pergerakan manusia di sekitar ruangan. Integrasi semua sensor ke dalam satu sistem berbasis ESP32 membuat proses pemantauan lebih efektif dan terpusat. Sensor PIR efektif dalam meningkatkan sistem pemantauan keamanan ruangan [13].

Selain meningkatkan keamanan akses, menggunakan Bot Telegram memudahkan pengguna untuk memantau ruangan dari jarak jauh. Pengguna dapat menerima informasi secara real-time ketika aktivitas mencurigakan terjadi tanpa harus hadir di lokasi. bahwa Bot Telegram efektif sebagai alat pemantauan keamanan berbasis *IoT* [6]. Hasil akhir dari penelitian menunjukkan bahwa sistem keamanan pintu otomatis yang dikembangkan stabil dan responsif. Sistem ini dapat secara otomatis membuka dan mengunci pintu, mendeteksi aktivitas mencurigakan, dan mengirimkan notifikasi waktu nyata kepada pengguna. Dengan konsep sistem satu gerbang, semua proses keamanan dan pemantauan dapat dilakukan secara terpusat dalam satu sistem terintegrasi. Penelitian ini juga mendukung penelitian Kurniasyah dan Rakhmawati (2024), yang menyatakan bahwa mengintegrasikan teknologi *IoT* ke dalam kunci pintu pintar dapat meningkatkan efisiensi pemantauan keamanan secara real-time. Berikut adalah foto dengan pemilik CV. Dua Sekawan Motor setelah melakukan tes dan validasi sistem, yang ditunjukan pada gambar 3.6 dibawah.

Gambar 13. Validasi Dengan Pemilik CV

4. KESIMPULAN

Penelitian ini berhasil merancang dan membangun sistem keamanan pintu otomatis berbasis *Internet of Things (IoT)* menggunakan ESP32, sensor sidik jari, sensor getaran SW-420, sensor PIR, dan Telegram Bot. Sistem ini mampu mengautentikasi akses pengguna, mendeteksi aktivitas mencurigakan, dan mengirimkan notifikasi waktu nyata kepada pengguna. Hasil tes menunjukkan bahwa semua komponen sistem berfungsi seperti yang diharapkan. Penggunaan beberapa sensor secara signifikan meningkatkan efektivitas keamanan dibandingkan dengan sistem konvensional yang hanya menggunakan kunci manual. Penelitian ini masih memiliki keterbatasan karena bergantung pada koneksi internet dan kurangnya sistem penyimpanan data berbasis cloud. Oleh karena itu, penelitian mendatang dapat mengembangkan sistem yang mengintegrasikan basis data cloud dan kamera CCTV untuk lebih meningkatkan keamanan.

DAFTAR PUSTAKA

[1] M. F. A. T. ANSYAH and S. Winardi, "Mesin Akses Ruangan Menggunakan Fingerprint Dan Rfid (Radio Frequency Identification) Berbasis Iot (Internet of Things)," *J. Pendidik. Teknol. Inf.*, vol. 5, no. 1, pp. 58–68, 2022, doi: 10.37792/jukanti.v5i1.443.

[2] P. Journal and O. F. Science, "Pengaman Pintu Dengan Sidik Jari Berbasis Arduino," vol. 2, no. 2, pp. 50–52, 2022.

[3] M. Hasan and Y. Turnandes, "Rancang Bangun Sistem Keamanan Pintu Ganda menggunakan Password dan Sidik Jari Berbasis Internet of Things (IoT)," *Prosiding-Seminar Nas. Teknol. Inf. Ilmu Komput.*, vol. 3, no. 1, pp. 221–237, 2024.

[4] Attariq Ziad, Eva Darnila, and Kurniawati, "Development and Implementation of an ESP32 Microcontroller and Monitoring System for Smart Door Lock Using RFID Sensor for E-KTP ID and Fingerprint Based on the Internet of Things," *Proc. Malikussaleh Int. Conf. Multidiscip. Stud.*, vol. 4, p. 00023, 2024, doi: 10.29103/micoms.v4i.908.

[5] D. M. Sepudin and S. Abdullah, "Sistem Keamanan Pintu Rumah Berbasis Internet of Things Berbasis NodeMCU ESP32 dan Telegram," *J. RESTIKOM Ris. Tek. Inform. dan Komput.*, vol. 4, no. 3, pp. 93–99, 2023, doi: 10.52005/restikom.v4i3.99.

[6] A. Febrianti, B. Nur Azizah, and E. Sulis Septiani, "Pemanfaatan Telegram Bot pada Sistem Keamanan Rumah Berbasis IoT dengan Mikrokontroler ESP32," *Pros. Semin. Nas. Teknol. Inf. dan Bisnis*, pp. 532–539, 2025, doi: 10.47701/jxxvgb60.

[7] R. Hermawan and A. Abdurrohman, "PEMANFAATAN TEKNOLOGI INTERNET OF THINGS PADA ALARM SEPEDA MOTOR MENGGUNAKAN NodeMcu LoLiN V3 DAN MEDIA TELEGRAM," *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 5, no. 2, p. 58, 2020, doi: 10.32897/infotronik.2020.5.2.453.

[8] G. A. Pangestu, Juwari, and M. Y. Asyhari, "Sistem Keamanan Rumah Berbasis Internet of Things (IoT) Menggunakan Notifikasi Bot Telegram untuk Pendeteksian Gerak," *J. Smart Syst.*, vol. 4, no. 1,

pp. 1–14, 2024, [Online]. Available: https://ejournal.utp.ac.id/index.php/JSS/article/view/3913

[9] M. Adonis and Slamet Winardi, "Rancang Bangun Smart Door Lock Berbasis Iot dan Recording Data Pada Firebase," *Modem J. Inform. dan Sains Teknol.*, vol. 3, no. 2, pp. 13–29, 2025, doi: 10.62951/modem.v3i2.384.

[10] M. N. Nizam, Haris Yuana, and Zunita Wulansari, "Mikrokontroler Esp 32 Sebagai Alat Monitoring Pintu Berbasis Web," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 6, no. 2, pp. 767–772, 2022, doi: 10.36040/jati.v6i2.5713.

[11] S. Suhaeb, U. Rahmah, and Agus, "Pengembangan Absensi Kehadiran Fingerprint Fpm10a DanCamera Esp32-Cam Di Jurusan Pendidikan Teknik ElektronikaFt-Unm," *Jetc*, vol. 16, 2021, [Online]. Available: https://ojs.unm.ac.id/JETC/article/download/29881/14012

[12] D. Desmira, D. Aribowo, W. D. Nugroho, and S. Sutarti, "Penerapan Sensor Passive Infrared (Pir) Pada Pintu Otomatis Di Pt Lg Electronic Indonesia," *PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 7, no. 1, 2020, doi: 10.30656/prosisko.v7i1.2123.

[13] Rouhillah, Inzar Salfikar, and Fajri Aqsalmi, "Implementasi Sensor PIR Dan Kamera Untuk Keamanan Ruangan Berbasis Internet of Things," *J-Innovation*, vol. 12, no. 1, pp. 20–24, 2023, doi: 10.55600/jipa.v12i1.177.

[14] A. Hafizh, N. Kholis, M. S. Zuhrie, and A. Widodo, "Prototype of Early Warning System for Home Door Security Based on IoT Using Piezoelectric Sensor," *Ina. Indones. J. Electr. Eletronics Eng.*, vol. 3, no. 2, pp. 56–62, 2020, doi: 10.26740/inajeee.v3n2.p56-62.

[15] H. Adi, Z. Putra, S. A. Sukarno, and P. M. Bandung, "Pendeteksian Dan Peringatan Gempa Bumi Berbasis Sw-420," *J. Inform. dan Tek. Elektro Terap.*, vol. 13, no. 2, pp. 82–90, 2025.

Jicom : Journal Information & Computer
Volume 4, Nomor 2, Juli 2026, hlm.138-146
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Implementasi Sistem Pembatasan Akses *Wi-Fi* Berbasis *Voucher Mikhmon* Menggunakan *Mikrotik*

Ahmad Aksyal Alma'arif *[1], Ade Sumaedi [2]

[1,2] Program Studi Sistem Komputer, Fakultas Ilmu Komputer, Universitas Pamulang
[1]ahmadaksyal24@gmail.com, [2]adesumaedi10093@unpam.ac.id

(Naskah masuk: *12 Februari 2026*, diterima untuk diterbitkan: *31 Juli 2026*)

Abstrak - Kebutuhan terhadap akses internet nirkabel yang andal terus meningkat seiring berkembangnya aktivitas digital masyarakat. Permasalahan yang sering muncul pada jaringan Wi-Fi skala kecil hingga menengah adalah penggunaan kata sandi bersama tanpa sistem autentikasi individual, yang menyebabkan sulitnya pengendalian pengguna, ketidakseimbangan pemanfaatan bandwidth, serta rendahnya tingkat keamanan jaringan. Penelitian ini berfokus pada perancangan dan penerapan sistem hotspot Wi-Fi berbasis voucher dengan memanfaatkan router wireless MikroTik RB952Ui-5ac2nd sebagai perangkat utama pengelola jaringan. Penelitian dilakukan menggunakan metode penelitian terapan dengan pendekatan deskriptif kualitatif melalui tahapan studi literatur, observasi lapangan, perancangan topologi jaringan, konfigurasi sistem, serta pengujian fungsional. Proses konfigurasi dilakukan menggunakan aplikasi Winbox, sedangkan pengelolaan dan pemantauan pengguna hotspot dilakukan melalui aplikasi Mikhmon. Hasil implementasi menunjukkan bahwa sistem hotspot berbasis voucher mampu mengatur hak akses pengguna secara individual, membatasi waktu penggunaan, serta mengelola bandwidth dengan lebih efektif. Penerapan sistem ini memberikan peningkatan pada aspek keamanan jaringan, kemudahan administrasi, dan kestabilan layanan internet. Dengan demikian, sistem hotspot voucher berbasis MikroTik dapat dijadikan solusi praktis dan efisien dalam manajemen jaringan Wi-Fi yang terkontrol dan berkelanjutan.

Kata Kunci : Pembatasan, Wi-Fi, Voucher, Mikhmon, Mikrotik

Abstract – The demand for reliable wireless internet access continues to rise alongside the growth of digital activities within the community. A common issue in small-to-medium-scale Wi-Fi networks is the use of shared passwords without individual authentication systems; this leads to difficulties in user control, unbalanced bandwidth utilization, and low network security levels. This research focuses on the design and implementation of a voucher-based Wi-Fi hotspot system using the MikroTik RB952Ui-5ac2nd wireless router as the primary network management device. The study employs an applied research method with a qualitative descriptive approach, encompassing literature review, field observation, network topology design, system configuration, and functional testing. Configuration was performed using the Winbox application, while hotspot user management and monitoring were handled via the Mikhmon application. Implementation results demonstrate that the voucher-based hotspot system effectively manages individual user access rights, limits usage time, and optimizes bandwidth allocation. Deploying this system enhances network security, simplifies administration, and improves internet service stability. Consequently, the MikroTik-based voucher hotspot system serves as a practical and efficient solution for managing controlled and sustainable Wi-Fi networks.

Keywords: Restrictions, Wi-Fi, Voucher, Mikhmon, MikroTik

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi, khususnya pada bidang jaringan komputer, telah membawa perubahan signifikan dalam cara masyarakat mengakses dan memanfaatkan internet. Jaringan nirkabel (wireless network) menjadi salah satu teknologi yang paling banyak digunakan karena kemudahan instalasi, fleksibilitas, serta dukungannya terhadap mobilitas pengguna. Layanan Wi-Fi kini tidak hanya digunakan pada lingkungan perusahaan atau institusi pendidikan, tetapi juga pada lingkungan rumahan, usaha kecil, dan penyedia layanan internet lokal.[1]

Pada jaringan Wi-Fi skala kecil hingga menengah, permasalahan yang sering muncul adalah

penggunaan satu kata sandi bersama tanpa adanya mekanisme autentikasi pengguna secara individual. Pola penggunaan seperti ini menyebabkan administrator jaringan kesulitan dalam mengontrol jumlah pengguna aktif, durasi akses internet, serta pembagian bandwidth secara adil. Dampak yang ditimbulkan antara lain menurunnya kualitas layanan, koneksi yang tidak stabil, serta meningkatnya risiko keamanan jaringan.[2]

Tidak adanya sistem monitoring yang memadai menyebabkan administrator kesulitan dalam mengawasi aktivitas pengguna jaringan, sehingga berpotensi menimbulkan penyalahgunaan akses internet, seperti penggunaan bandwidth berlebihan, akses ke konten yang tidak diinginkan, serta penggunaan jaringan oleh pihak yang tidak berwenang. Router MikroTik menyediakan fitur hotspot yang memungkinkan penerapan autentikasi sebelum pengguna dapat mengakses internet melalui sistem voucher, di mana hak akses pengguna dapat diatur secara individual berdasarkan durasi, kecepatan, dan masa aktif. Integrasi dengan aplikasi Mikhmon sebagai alat manajemen dan monitoring hotspot memudahkan pembuatan voucher, pemantauan pengguna aktif, serta pengelolaan jaringan secara real-time. Penelitian ini bertujuan merancang dan mengimplementasikan sistem pembatasan akses Wi-Fi berbasis voucher menggunakan MikroTik dan Mikhmon pada jaringan ABI NET guna meningkatkan keamanan jaringan, menciptakan keadilan pemanfaatan bandwidth, serta mempermudah pengelolaan jaringan secara efektif dan efisien.[3]

II. LANDASAN TEORI

Landasan teori merupakan dasar konseptual yang digunakan untuk mendukung pelaksanaan penelitian secara ilmiah. Landasan teori berfungsi untuk menjelaskan konsep, prinsip, serta mekanisme yang berkaitan dengan permasalahan penelitian, sehingga pembahasan dan solusi yang dihasilkan memiliki dasar keilmuan yang jelas dan sistematis.

1. Jaringan Komputer

Jaringan Komputer didefinisikan sebagai sekumpulan perangkat komputasi yang saling terhubung melalui media komunikasi, baik kabel maupun nirkabel, untuk melakukan pertukaran data dan berbagi sumber daya secara terkoordinasi, di mana perangkat tersebut dapat berupa komputer, router, switch, access point, serta perangkat pengguna seperti laptop dan smartphone. Pembangunan jaringan komputer bertujuan meningkatkan efisiensi komunikasi, mempercepat distribusi informasi, serta mengoptimalkan pemanfaatan sumber daya bersama seperti koneksi internet dan perangkat keras. Dalam konteks layanan internet, jaringan komputer berperan sebagai infrastruktur utama yang menghubungkan pengguna dengan sumber informasi global serta memungkinkan pengelolaan akses, keamanan, dan kualitas layanan secara terpusat. Pada ABI NET, jaringan komputer dimanfaatkan untuk mengintegrasikan modem ISP, router MikroTik, pemancar Wi-Fi, dan perangkat pengguna dalam satu sistem yang saling terhubung. Permasalahan umum pada jaringan Wi-Fi skala kecil hingga menengah adalah belum adanya pengaturan akses pengguna yang terstruktur, seperti penggunaan satu kata sandi bersama tanpa autentikasi individual, yang berdampak pada ketidakseimbangan pembagian bandwidth dan potensi penyalahgunaan jaringan. Oleh karena itu, penerapan sistem pembatasan akses berbasis voucher memungkinkan jaringan komputer tidak hanya menghubungkan perangkat, tetapi juga mengatur, membatasi, dan memantau aktivitas pengguna melalui pengendalian durasi akses, kecepatan koneksi, serta jumlah pengguna aktif. Dengan demikian, jaringan komputer dipahami sebagai sistem terintegrasi yang mencakup pengelolaan akses, keamanan, dan kualitas layanan, serta menjadi landasan utama dalam perancangan dan implementasi sistem pembatasan akses Wi-Fi berbasis voucher menggunakan router MikroTik.[4]

2. *MikroTik RouterOS*

MikroTik merupakan perusahaan penyedia perangkat jaringan asal Latvia yang didirikan pada tahun 1996 dan dikenal sebagai pengembang perangkat keras serta perangkat lunak jaringan yang banyak digunakan pada pengelolaan jaringan skala kecil hingga menengah. Produk utama MikroTik adalah RouterOS, yaitu sistem operasi berbasis Linux yang dirancang untuk kebutuhan routing, firewall, manajemen bandwidth, dan pengelolaan jaringan secara menyeluruh, yang dapat diinstal pada komputer umum maupun perangkat khusus RouterBOARD. RouterOS menyediakan berbagai fitur seperti pengaturan alamat IP, NAT, firewall, manajemen bandwidth, serta layanan hotspot yang mendukung autentikasi pengguna, dan dapat dikonfigurasi melalui antarmuka grafis menggunakan Winbox maupun baris perintah. Dalam penelitian ini, MikroTik RouterOS digunakan sebagai komponen inti dalam penerapan sistem pembatasan akses internet berbasis voucher pada ABI NET, di mana fitur hotspot memungkinkan

Jicom : Journal Information & Computer
Volume 4, Nomor 2, Juli 2026, hlm.138-146
DOI : 10.32493/jicomisc.v2i1.37666
P-ISSN : 3031-2779
E-ISSN : 3026-4197

pengguna melakukan autentikasi melalui halaman login sebelum memperoleh akses internet. Selain itu, RouterOS mendukung pengaturan profil pengguna sesuai jenis voucher, termasuk pembatasan durasi akses dan kecepatan koneksi, sehingga pembagian bandwidth menjadi lebih adil dan terkontrol. Integrasi RouterOS dengan aplikasi Mikhmon juga mempermudah proses manajemen dan monitoring jaringan, seperti pembuatan voucher dan pemantauan pengguna aktif, sehingga seluruh aktivitas jaringan dapat dikelola secara terpusat dan sistem hotspot dapat berjalan secara efektif dan efisien.[5]

Gambar 1.*Router Mikrotik* RB952Ui-5ac2nd

3. *Hotspot*

Hotspot merupakan layanan jaringan nirkabel yang memungkinkan pengguna terhubung ke internet melalui mekanisme autentikasi tertentu sebelum memperoleh hak akses. Mekanisme autentikasi ini berfungsi sebagai sistem pengendalian agar penggunaan jaringan tidak dilakukan secara bebas tanpa batasan. Penerapan hotspot memungkinkan administrator jaringan untuk mengatur hak akses pengguna, membatasi durasi penggunaan, serta menjaga kestabilan koneksi jaringan. Dalam pengelolaan jaringan komputer hotspot berperan sebagai penghubung antara pengguna dan jaringan internet yang dikendalikan secara terpusat. Melalui sistem ini, setiap aktivitas pengguna dapat diatur berdasarkan kebijakan tertentu, seperti pembatasan waktu akses dan pengendalian kecepatan koneksi. Penerapan hotspot dinilai efektif dalam mengontrol penggunaan jaringan, baik pada lingkungan publik maupun lingkungan rumahan yang memiliki jumlah pengguna beragam. Kaitan dengan penelitian ini hotspot digunakan sebagai komponen utama dalam penerapan pembatasan akses jaringan Wi-Fi di ABI NET. Dengan memanfaatkan fitur hotspot pada router MikroTik, proses autentikasi pengguna dapat dilakukan secara individual sehingga akses jaringan menjadi lebih tertib, terkontrol, dan sesuai dengan kapasitas layanan *internet* yang tersedia.[6]

4. Sistem *Voucher*

Sistem *voucher* merupakan metode autentikasi jaringan yang menggunakan kode akses unik sebagai syarat untuk memperoleh layanan internet, di mana setiap voucher memiliki batasan tertentu seperti durasi penggunaan, kuota, atau kecepatan akses sehingga hak akses pengguna dapat dikendalikan secara terstruktur. Sistem ini banyak diterapkan pada layanan hotspot karena fleksibel dan memungkinkan pengelolaan akses pengguna secara individual, sehingga lebih efektif dibandingkan penggunaan satu kata sandi bersama. Penerapan sistem voucher bertujuan menciptakan keadilan dalam pemanfaatan jaringan dengan membatasi penggunaan bandwidth sesuai kebijakan yang ditetapkan serta meminimalkan potensi penyalahgunaan jaringan. Dalam penelitian ini, sistem voucher diterapkan pada jaringan Wi-Fi ABI NET melalui integrasi hotspot pada router MikroTik, di mana pengguna diwajibkan memasukkan kode voucher yang valid untuk memperoleh akses internet sesuai profil yang telah ditentukan, sehingga diharapkan mampu meningkatkan keteraturan, stabilitas layanan, dan kemudahan pengelolaan jaringan.[7]

5. *Winbox*

Winbox merupakan aplikasi berbasis antarmuka grafis yang dikembangkan oleh MikroTik untuk memudahkan konfigurasi dan manajemen perangkat MikroTik RouterOS tanpa menggunakan perintah baris teks. Winbox dirancang agar proses konfigurasi jaringan dapat dilakukan secara lebih cepat, mudah, dan efisien melalui menu yang terstruktur dan tampilan yang intuitif. Dalam penelitian ini, Winbox digunakan sebagai alat utama untuk melakukan konfigurasi router MikroTik pada sistem hotspot berbasis voucher, meliputi pengaturan IP Address, layanan hotspot, bridge, antarmuka jaringan, serta kebijakan keamanan seperti firewall. Penggunaan Winbox memungkinkan seluruh proses konfigurasi dan pengelolaan jaringan dilakukan secara terpusat, sehingga mendukung terciptanya sistem jaringan Wi-Fi yang lebih aman, terintegrasi, dan efisien sesuai dengan tujuan penelitian.[8]

6. *Monitoring* Jaringan dengan *Mikhmon*

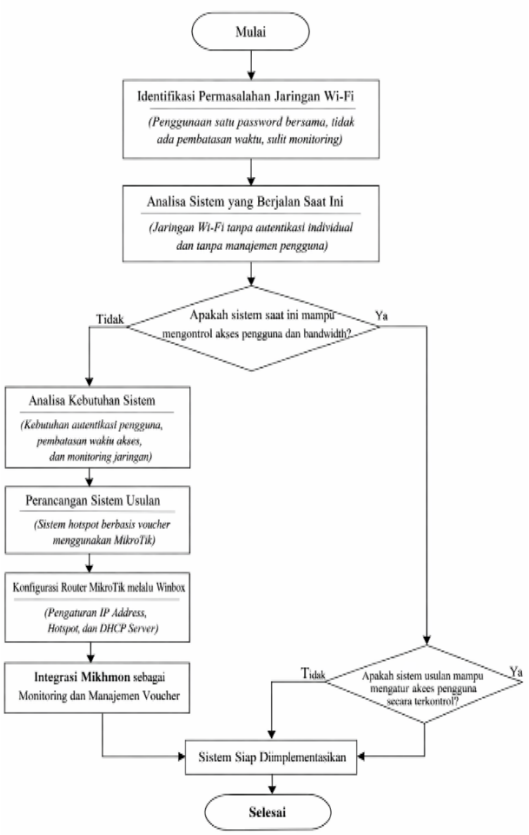
Mikhmon (MikroTik Hotspot Monitor) merupakan aplikasi berbasis web yang terintegrasi dengan MikroTik

RouterOS untuk membantu administrator jaringan dalam membuat, mengelola, dan memonitor voucher hotspot secara terpusat. Aplikasi ini menyediakan fitur pembuatan voucher massal dengan pengaturan durasi akses, pembatasan bandwidth, dan harga voucher, serta fasilitas monitoring aktivitas pengguna secara real-time. penggunaan Mikhmon dapat meningkatkan efisiensi administrasi sistem billing hotspot karena memudahkan pencatatan penggunaan voucher, pemantauan pengguna aktif, dan pengelolaan laporan jaringan tanpa perlu konfigurasi manual melalui RouterOS. Dalam penelitian ini, Mikhmon digunakan sebagai alat utama monitoring jaringan Wi-Fi berbasis voucher pada ABI NET untuk memantau jumlah pengguna aktif, durasi penggunaan, dan status koneksi, sehingga membantu menjaga stabilitas layanan serta mempermudah pengelolaan jaringan dengan jumlah pengguna yang relatif banyak.[9]

III. METODOLOGI PENELITIAN

1. Analisa Sistem

Analisa sistem merupakan tahapan penting dalam penelitian yang bertujuan untuk memperoleh pemahaman menyeluruh terhadap sistem yang dikaji dengan menguraikan elemen sistem, hubungan antar komponen, mekanisme kerja, serta permasalahan yang terjadi pada sistem berjalan. Analisa sistem pada penelitian ini disesuaikan dengan permasalahan pada latar belakang, yaitu belum adanya pengelolaan akses jaringan Wi-Fi yang terstruktur, penggunaan satu kata sandi secara bersama, serta ketiadaan mekanisme autentikasi pengguna, yang berdampak pada sulitnya pengendalian jumlah pengguna, durasi akses, dan pembagian bandwidth secara adil. Oleh karena itu, pendekatan eksperimental digunakan karena sistem tidak hanya dianalisis secara teoritis, tetapi juga dirancang, diimplementasikan, dan diuji langsung pada perangkat jaringan untuk mengevaluasi apakah sistem hotspot berbasis voucher menggunakan MikroTik mampu mengatasi permasalahan sebelumnya dan berjalan sesuai dengan tujuan penelitian.



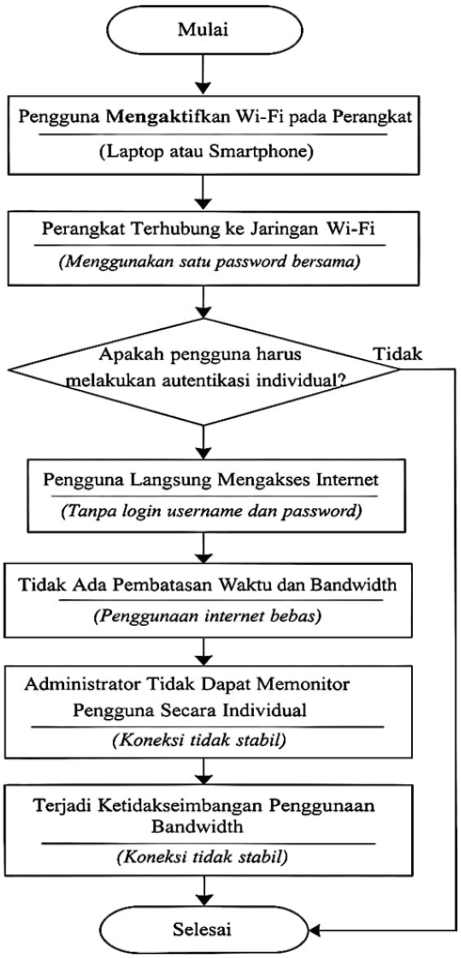
Gambar 2. *Flowchart* Analisa Sistem

2. Analisa Sistem Saat Ini

Analisa sistem saat ini merupakan proses untuk mempelajari, memahami, dan mendokumentasikan kondisi jaringan yang sedang berjalan sebelum dilakukan perancangan sistem usulan. Pada penelitian ini, sistem yang dianalisis adalah jaringan Wi-Fi rumahan yang masih menggunakan konfigurasi standar dari modem ISP tanpa manajemen pengguna yang terstruktur, di mana pengguna dapat langsung terhubung ke jaringan hanya dengan satu kata sandi bersama tanpa autentikasi individual. Kondisi tersebut menyebabkan pengelola jaringan kesulitan dalam mengendalikan jumlah pengguna aktif, membatasi durasi akses, serta mengatur pemanfaatan bandwidth secara

Jicom : Journal Information & Computer
Volume 4, Nomor 2, Juli 2026, hlm.138-146
DOI : 10.32493/jicomisc.v2i1.37666
P-ISSN : 3031-2779
E-ISSN : 3026-4197

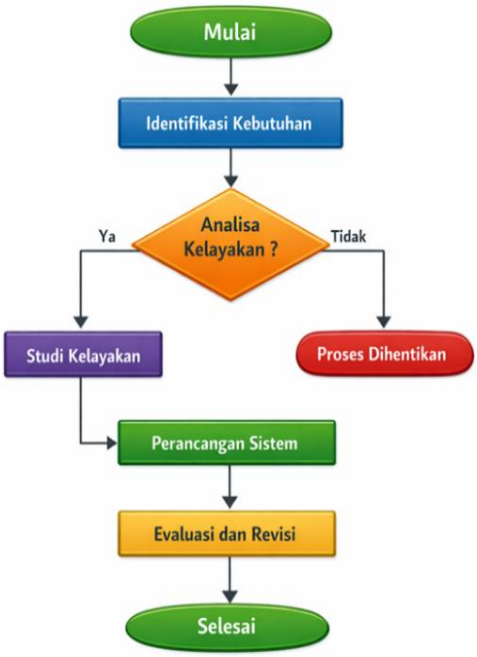
optimal karena tidak adanya pengaturan prioritas dan pembatasan penggunaan. Oleh karena itu, analisa sistem saat ini dilakukan sebagai langkah awal untuk memperoleh gambaran nyata kondisi jaringan di lapangan, sehingga perancangan sistem usulan dapat disesuaikan dengan permasalahan yang ada dan diharapkan mampu meningkatkan keteraturan akses, efektivitas pengelolaan jaringan, serta kestabilan layanan internet.



Gambar 3. *Flowchart* Analisa Sistem Saat Ini

3. Analisa Sistem Usulan

Analisa sistem usulan merupakan proses untuk mempelajari dan mengevaluasi rancangan sistem baru yang di-usulkan sebagai solusi atas permasalahan pada sistem sebelumnya. Sistem usulan dalam penelitian ini adalah penerapan jaringan hotspot berbasis MikroTik dengan konfigurasi menggunakan Winbox serta monitoring pengguna melalui Mikhmon. Pada sistem usulan, pengguna diwajibkan melakukan proses login menggunakan akun hotspot atau voucher sebelum dapat mengakses internet. Dengan penerapan sistem ini, pengelolaan pengguna menjadi lebih terstruktur, pembagian bandwidth dapat diatur dengan baik, serta aktivitas pengguna dapat dimonitor secara real-time. Sistem usulan diharapkan mampu meningkatkan keamanan, efisiensi, dan kualitas layanan jaringan Wi-Fi rumahan.



Gambar 4. *Flowchart* Analisa Sistem Usulan

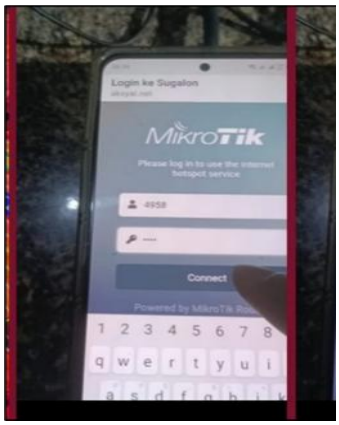
4. Teknik Pengumpulan Data

   Teknik pengumpulan data dalam penelitian ini meliputi:

   1. Observasi dilakukan dengan cara melakukan pengamatan langsung terhadap kondisi jaringan Wi-Fi yang berjalan, meliputi topologi jaringan, mekanisme akses pengguna, penggunaan bandwidth, serta permasalahan yang muncul seperti penggunaan satu kata sandi secara bersama dan tidak adanya pengelolaan akses yang terstruktur. Hasil observasi digunakan sebagai dasar dalam analisa sistem dan perancangan sistem hotspot berbasis voucher.
   2. Studi pustaka dilakukan dengan mengumpulkan dan mempelajari berbagai referensi yang relevan, seperti buku teks, jurnal ilmiah, prosiding, dan sumber daring terpercaya yang berkaitan dengan jaringan komputer, hotspot MikroTik, sistem autentikasi, manajemen bandwidth, serta penggunaan voucher. Studi pustaka bertujuan untuk memperoleh landasan teori yang mendukung penelitian serta memperkuat analisa dan perancangan sistem.
   3. Dokumentasi dilakukan dengan mencatat dan menyimpan seluruh proses konfigurasi, implementasi, dan pengujian sistem hotspot berbasis MikroTik. Dokumentasi meliputi hasil konfigurasi melalui Winbox, pembuatan akun atau voucher, monitoring pengguna menggunakan Mikhmon, serta hasil pengujian kinerja sistem. Data dokumentasi digunakan sebagai bukti pendukung dan bahan evaluasi terhadap keberhasilan sistem yang diusulkan.

5. Teknik Pengujian Sistem

Pengujian sistem dilakukan untuk memastikan *hotspot* berfungsi sesuai perancangan. Pengujian dilakukan menggunakan *handphone* dengan mencoba koneksi *Wi-Fi*, apabila berhasil, perangkat terhubung ke jaringan internet sesuai *voucher* yang digunakan.



Gambar 5. Tampilan Login Page pada Handphone

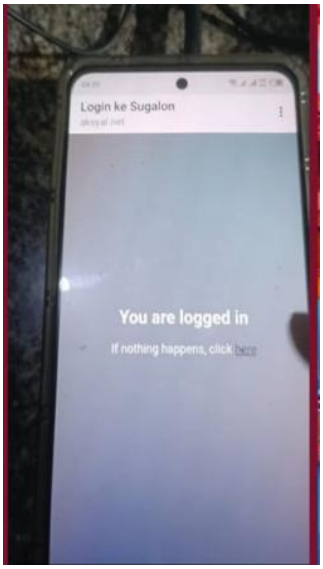
Jicom : Journal Information & Computer
Volume 4, Nomor 2, Juli 2026, hlm.138-146
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

IV. HASIL DAN PEMBAHASAN

1. Hasil Perancangan

Hasil perancangan pada penelitian ini berupa sistem pembatasan akses Wi-Fi berbasis voucher yang diimplementasikan menggunakan router MikroTik sebagai pusat pengelolaan jaringan. Sistem dirancang agar setiap pengguna yang terhubung ke jaringan Wi-Fi tidak dapat langsung mengakses internet sebelum melalui proses autentikasi pada halaman login hotspot dengan memasukkan kode voucher yang telah dibuat oleh administrator. Berdasarkan topologi jaringan, sistem terdiri atas modem ISP sebagai sumber koneksi internet, router MikroTik yang dikonfigurasikan menggunakan aplikasi Winbox dengan mode AP Bridge atau Bridge, serta perangkat pengguna berupa laptop dan smartphone. Koneksi internet dari modem ISP diteruskan ke router MikroTik untuk dikelola dan didistribusikan kepada pengguna, di mana MikroTik berperan sebagai pusat pengaturan layanan hotspot, termasuk pengelolaan alamat IP, autentikasi pengguna, serta pembatasan akses internet. Saat perangkat pengguna pertama kali terhubung ke jaringan, sistem secara otomatis mengarahkan pengguna ke halaman login hotspot, dan akses internet hanya diberikan apabila voucher yang dimasukkan valid sesuai dengan ketentuan waktu dan bandwidth yang telah dikonfigurasikan. Perancangan sistem ini bertujuan untuk memudahkan administrator dalam mengelola pengguna jaringan serta memastikan penggunaan internet lebih terkontrol, adil, dan stabil melalui pengaturan akses yang terstruktur pada router MikroTik.



Gambar 6. Tampilan Akses Internet Berhasil Setelah *Login Voucher*

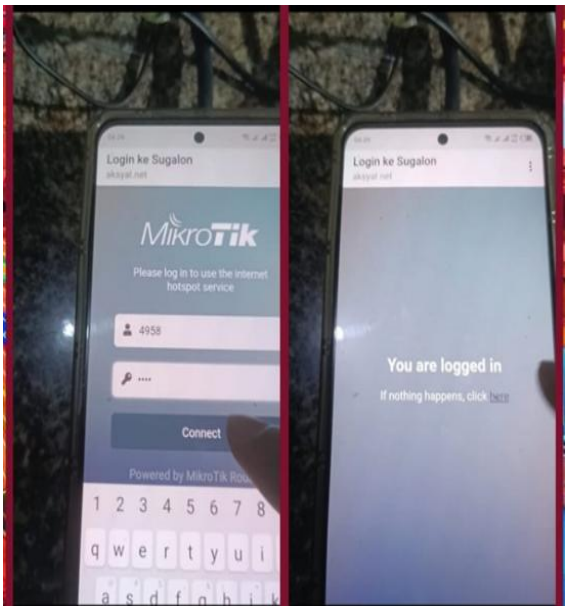
Tabel 1. Perbandingan Kondisi Jaringan Sebelum dan Sesudah Implementasi

No	Parameter Analisis	Sistem Lama (Konven-sional)	Sistem Baru (Usulan)
1	Mekanisme Autentikasi	Satu kata sandi untuk semua pengguna (shared password)	*Login Page* dengan Kode *Voucher* unik per pengguna
2	Pembata-san Waktu	Tidak ada pembatasan waktu penggunaan	Akses di-batasi ber-dasarkan durasi pada *voucher*

No	Parameter Analisis	Sistem Lama (Konvensional)	Sistem Baru (Usulan)
3	Manajemen *Bandwidth*	Tidak teratur, berpotensi menurunkan stabilitas	Teratur melalui fitur Rate Limit pada profil pengguna
4	Pemantauan Pengguna	Tidak tersedia sistem monitoring efektif	Monitoring real-time menggunakan aplikasi *Mikhmon*
5	Keamanan Jaringan	Lemah, potensi penyalahgunaan akses tinggi	Lebih aman dengan autentikasi individu

2. Hasil Implementasi

Tahap implementasi merupakan perwujudan dari seluruh konfigurasi yang telah dilakukan sebelumnya pada *Router MikroTik* menggunakan *Winbox* dan manajemen *voucher* melalui *Mikhmon*. Hasil implementasi ini menunjukkan bagaimana sistem bekerja saat diakses oleh pengguna di lokasi penelitian (ABI NET).



Gambar 7. Tampilan *Login Page* pada Perangkat Pengguna Setelah berhasil mendapatkan internet

V. KESIMPULAN DAN SARAN

1. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa implementasi pembatasan akses *Wi-Fi* berbasis *voucher* menggunakan *router MikroTik* berhasil diterapkan dengan baik. Sistem *hotspot* yang dibangun mampu membatasi akses pengguna melalui mekanisme login *voucher* sehingga pengguna tidak dapat mengakses internet secara bebas tanpa autentikasi. Penggunaan *Mikhmon* mempermudah pengelolaan *voucher*, mulai dari pengaturan masa aktif, pembatasan *bandwidth*, hingga manajemen pengguna. Dengan penerapan sistem ini, pengelolaan jaringan *Wi-Fi* menjadi lebih terkontrol, aman, dan efektif sesuai dengan tujuan penelitian.

2. SARAN

Berdasarkan hasil penelitian yang telah dilakukan, disarankan agar sistem pembatasan akses *Wi-Fi* berbasis *voucher* ini dapat dikembangkan lebih lanjut. Pengembangan dapat dilakukan dengan menambahkan variasi paket *voucher* yang lebih beragam, pengaturan *bandwidth* yang lebih detail, serta peningkatan keamanan jaringan. Selain

P-ISSN : 3031-2779
E-ISSN : 3026-4197

itu, sistem ini dapat diterapkan pada skala jaringan yang lebih luas agar manfaatnya dapat dirasakan oleh lebih banyak pengguna, baik sebagai bahan pengembangan penelitian selanjutnya maupun sebagai solusi praktis dalam pengelolaan jaringan *Wi-Fi*

VI. DAFTAR PUSTAKA

[1] D. Wahyudi, A. K. Nalendra, Muhammad Ivan Wahyudi, and Heni Puji Lestari, "PENERAPAN SISTEM VOUCHER PADA JARINGAN RT/RW-NET MENGGUNAKAN MIKHMON," *JAMI: Jurnal Ahli Muda Indonesia*, vol. 3, no. 1, pp. 51–60, Jun. 2022, doi: 10.46510/jami.v3i1.95.

[2] U. A. Pringsewu, P. Konfigurasi, J. Hotspot, D. V. Wifi, and I. Awaliyani, "Aisyah Journal of Informatics and Electrical Engineering", [Online]. Available: http://jti.aisyahuniversity.ac.id/index.php/AJIEE

[3] M. Mujahiddin, A. Wahid, and J. Parenreng, "Sistem Manajemen Voucher Wifi Untuk Jaringan di Pedesaan Dengan Menggunakan Teknologi Mikrotik Dan Mikhmon," *Jurnal Komputer, Informasi dan Teknologi*, vol. 5, no. 1, p. 18, Feb. 2025, doi: 10.53697/jkomitek.v5i1.2263.

[4] R. Dian Candra Wirlaksana, A. Sumaedi, and N. Huda, "IMPLEMENTASI SISTEM HOTSPOT MIKROTIK SEBAGAI UPAYA PEMERATAAN JARINGAN INTERNET DI PEDESAAN IMPLEMENTATION OF PROXY HOTSPOT SYSTEM AS AN EFFORT TO EQUALISE INTERNET NETWORK IN RURAL AREAS," *Pengabdian Kepada Masyarakat*, vol. 2, no. 5, 2024.

[5] "466794-none-7a5a4b17".

[6] D. Wahyudi, A. K. Nalendra, Muhammad Ivan Wahyudi, and Heni Puji Lestari, "PENERAPAN SISTEM VOUCHER PADA JARINGAN RT/RW-NET MENGGUNAKAN MIKHMON," *JAMI: Jurnal Ahli Muda Indonesia*, vol. 3, no. 1, pp. 51–60, Jun. 2022, doi: 10.46510/jami.v3i1.95.

[7] E. Eben, M. Mukramin, and H. Abduh, "PENGEMBANGAN MANAJEMEN KEAMANAN JARINGAN NIRKABEL (WIFI) MENGGUNAKAN ROUTERBOARD MIKROTIK DAN FIREWALL PADA SMK KRISTEN PALOPO," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 12, no. 3, Aug. 2024, doi: 10.23960/jitet.v12i3.4716.

[8] P. Konfigurasi Hotspot Dan Voucher Login, R. Taufiq Subagio, W. Ilham, and I. Romadon, "MENGGUNAKAN MIKROTIK RB952ui DENGAN WEB TOP UP PADA NORALONA COFFEE ROASTERY," *Ridho Taufiq Subagio*, vol. 1, no. 2.

[9] T. Setiadi and D. G. Saputra, "Perancangan Jaringan Hotspot Di Smk Muhammadiyah 3 Weleri Menggunakan Mikrotik Dengan Server Proxy Eksternal," *JURNAL ILMIAH SISTEM INFORMASI (JUSI)*, vol. 1, no. 3, pp. 7–13, 2022, [Online]. Available: http://ejurnal.provisi.ac.id/index.php/JUISI□page7

JOURNAL
INFORMATION & COMPUTER

sinta 4
Science and Technology Index

JICOM
E-ISSN 3026-4197
P-ISSN 3031-2779

ISSN 3026-4197
ISSN 3031-2779

Alamat Redaksi: Jl. Lintas Serang - Jakarta Kampung Limandang, Kelurahan Kelodran, Kecamatan Walantaka Kota Serang Banten, Telp/WA. +62818-1899-3063 Email: ojsjicom@unpam.ac.id