Journal of Information System Research (JOSH)
Volume 7, No. 4, Juli 2026, pp 903−913
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i4.9205

Peningkatan Keamanan Kunci Vigenère Menggunakan Steganografi Least Significant Bit (LSB) pada Sistem IoT Smart Door QR Code

Kasliono*, Syamsul Bahri, Dwi Marisa Midyanti, Muhammad Dito Asrofa, Riski Arasyid

Fakultas Matematika dan Ilmu Pengetahuan Alam, Program Studi Rekayasa Sistem Komputer, Universitas Tanjungpura, Pontianak
Jl. Profesor Dokter H. Hadari Nawawi, Bansir Laut, Kec. Pontianak Tenggara, Kota Pontianak, Kalimantan Barat, Indonesia
Email: [1]*kasliono@siskom.untan.ac.id, [2]syamsul.bahri@siskom.untan.ac.id, [3]dwi.marisa@siskom.untan.ac.id,
[4]h1051211005@student.untan.ac.id, [5]h1051211025@student.untan.ac.id
Email Penulis Korespondensi: kasliono@siskom.untan.ac.id
Submitted: **14/01/2026**; Accepted: **30/06/2026**; Published: **05/07/2026**

Abstrak−Dalam era digital yang semakin terhubung, Internet of Things (IoT) menghadirkan kemudahan dalam pertukaran data antar perangkat secara real-time, namun juga menimbulkan tantangan besar dalam aspek keamanan data. Kriptografi simetri banyak digunakan karena efisiensi komputasinya, tetapi distribusi dan perlindungan kunci masih menjadi permasalahan utama. Penelitian ini bertujuan untuk meningkatkan keamanan jaringan IoT dengan mengintegrasikan kriptografi Vigenère Cipher dan steganografi Least Significant Bit (LSB). Metode LSB digunakan untuk menyembunyikan kunci kriptografi dalam media digital sehingga mengurangi risiko pencurian kunci oleh pihak tidak berwenang. Sistem diuji pada tiga jalur komunikasi data, yaitu server, web pengguna, dan perangkat ESP32/ESP32-CAM. Hasil pengujian serangan sniffing menunjukkan bahwa seluruh data terkirim dalam bentuk ciphertext yang berbeda dari plaintext aslinya, menandakan keberhasilan penerapan kedua metode dalam menjaga kerahasiaan data. Proses enkripsi dan encode di sisi pengirim serta decode dan dekripsi di sisi penerima juga menunjukkan kinerja yang cepat, dengan rata-rata waktu di server sebesar 0,14 ms untuk enkripsi dan encode, serta 0,13 ms untuk decode dan dekripsi di web pengguna. Pada ESP32-CAM, waktu rata-rata untuk enkripsi dan encode adalah 2,22 ms, sedangkan decode dan dekripsi di server memerlukan 0,10 ms. Sementara itu, pada ESP32, proses enkripsi dan encode dilakukan di server dengan waktu 0,10 ms, sedangkan decode dan dekripsi di ESP32 memerlukan waktu 1,46 ms. Secara keseluruhan, integrasi kedua metode tersebut terbukti efektif meningkatkan keamanan komunikasi data tanpa mengurangi performa sistem secara signifikan.

Kata Kunci: Steganografi; Kriptografi Simetri; Vigenère Cipher; Keamanan IoT; Least Significant Bit ;Pintu Cerdas

Abstract−In an increasingly connected digital era, the Internet of Things (IoT) enables seamless real-time data exchange across devices but also introduces critical challenges in data security. Although symmetric cryptography is widely adopted for its computational efficiency, key distribution and protection remain major vulnerabilities. This study aims to enhance IoT network security by integrating the Vigenère Cipher with Least Significant Bit (LSB) steganography. The LSB method is employed to conceal cryptographic keys within digital media, reducing the risk of unauthorized key interception. The proposed system is evaluated across three communication channels: the server, the user web interface, and ESP32/ESP32-CAM devices. Sniffing attack tests confirm that all transmitted data appears only as ciphertext, indicating successful protection of plaintext and secure key exchange. Performance measurements also demonstrate that the combined methods operate efficiently. On the server, encryption and encode require an average of 0.14 ms, while decode and decryption on the user web interface require 0.13 ms. On the ESP32-CAM, encryption and encode average 2.22 ms, with decode and decryption on the server requiring 0.10 ms. For the ESP32, server-side encryption and encode take 0.10 ms, while device-side decode and decryption take 1.46 ms. Overall, the integration of Vigenère Cipher and LSB steganography effectively improves data security in IoT communication without significantly impacting system performance.

Keywords: Steganography; Symmetric Cryptography; Vigenère Cipher; IoT Security; Least Significant Bit (LSB); Smart Door

1. PENDAHULUAN

Perkembangan teknologi Internet of Things (IoT) memungkinkan objek fisik saling terhubung melalui jaringan internet sehingga mampu berkomunikasi dan bertukar informasi secara otomatis serta real-time [1]. IoT telah banyak diterapkan pada berbagai bidang, termasuk sistem keamanan rumah seperti Smart Door lock, yang memungkinkan proses membuka dan mengunci pintu dilakukan tanpa kunci fisik, melainkan melalui perangkat elektronik yang terhubung ke internet [2]. Salah satu jenis Smart Door yang banyak digunakan adalah sistem berbasis Quick Response (QR) Code, yaitu barcode dua dimensi yang mampu menyimpan data dalam jumlah besar dan dapat dipindai dengan cepat [3]. Dengan integrasi IoT, Smart Door berbasis QR Code memungkinkan pemilik properti memonitor akses pintu secara real-time, meningkatkan keamanan, dan memberikan fleksibilitas dalam manajemen akses penghuni.

Meskipun menawarkan kemudahan, sistem Smart Door berbasis QR Code menghadapi tantangan serius dalam aspek keamanan data. Komunikasi antara perangkat seperti website pengguna, server, ESP-CAM, dan ESP32 sering kali tidak dilengkapi lapisan enkripsi yang memadai. Kondisi ini menyebabkan sistem rentan terhadap serangan Man-in-the-Middle (MitM), di mana penyerang dapat menyadap dan memanipulasi data autentikasi untuk mendapatkan akses ilegal [4]. Ancaman ini semakin relevan mengingat penelitian menunjukkan bahwa sekitar 98% lalu lintas perangkat IoT tidak dienkripsi [5]. Salah satu bentuk serangan MitM yang umum terjadi adalah sniffing, yaitu teknik penyadapan paket data dalam jaringan, baik kabel maupun nirkabel,

Journal of Information System Research (JOSH)
Volume 7, No. 4, Juli 2026, pp 903−913
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i4.9205

menggunakan perangkat maupun perangkat lunak khusus [6]. Serangan seperti ini sangat berbahaya mengingat Smart Door merupakan sistem keamanan fisik yang berhubungan langsung dengan keselamatan penghuni.

Untuk menjaga kerahasiaan dan integritas data pada perangkat IoT, kriptografi digunakan sebagai mekanisme utama selama proses transmisi. Pendekatan berbasis kunci simetris dipilih karena prosesnya ringan dan tidak membutuhkan banyak sumber daya, sehingga sesuai untuk perangkat berdaya rendah, termasuk mikrokontroler seperti ESP32 dan ESP8266 [7]. Salah satu algoritma yang relevan adalah Vigenère Cipher yang merupakan algoritma kriptografi simetris yang mengamankan pesan teks melalui gabungan beberapa sandi Caesar yang membentuk pola substitusi berbasis deretan alfabet [8]. Namun, tantangan utama pada kriptografi simetri terletak pada proses distribusi kunci yang harus dilakukan secara aman. Kelemahan dalam tahap ini dapat membuka peluang bagi pihak tidak berwenang untuk mendapatkan kunci dan mengakses seluruh data yang dilindungi [9].

Steganografi dapat digunakan sebagai lapisan tambahan untuk menyembunyikan kunci dengan menempatkannya ke dalam media lain agar tidak mudah terdeteksi. Teknik yang sering digunakan adalah Least Significant Bit (LSB), yaitu penyisipan data dengan mengubah bit paling tidak signifikan pada sebuah file sehingga perubahan yang terjadi hampir tidak terlihat [10]. LSB sangat cocok diterapkan pada sistem IoT karena proses penyisipannya ringan dan tidak menimbulkan perubahan signifikan pada media yang digunakan. Dengan menyisipkan ciphertext ke dalam media melalui teknik ini, informasi yang dikirim menjadi jauh lebih sulit dideteksi atau diidentifikasi oleh penyerang selama proses distribusi.

Beberapa penelitian sebelumnya telah mengembangkan sistem Smart Door berbasis QR Code maupun penggunaan Vigenère Cipher untuk pengamanan data. Basit et al. (2022) merancang sistem keamanan pintu otomatis berbasis QR Code menggunakan Raspberry Pi dan Pi Camera, namun belum menyertakan mekanisme pengamanan kunci enkripsi [11]. Murni et al. (2023) menerapkan Vigenère Cipher untuk pengamanan pesan pada aplikasi web, tetapi penelitian tersebut tidak berfokus pada distribusi kunci aman serta tidak diterapkan dalam sistem IoT [12]. Selanjutnya, Rachmawanto et al. (2023) menerapkan Vigenère Cipher untuk keamanan data pada QR Code, namun masih sebatas enkripsi langsung tanpa integrasi teknik steganografi [13]. Penelitian lain oleh Umam et al. (2022) menggabungkan steganografi LSB dan algoritma kriptografi AES untuk mengamankan pesan teks pada citra berwarna, namun penelitian ini masih berfokus pada keamanan pesan umum dan belum diterapkan pada konteks distribusi kunci sistem IoT Smart Door [14]. Selain itu, Harahap dan Hasugian (2023) menerapkan kombinasi Vigenère Cipher dan steganografi LSB untuk penyisipan pesan pada citra, tetapi penelitian tersebut tidak diarahkan untuk pengamanan kunci pada arsitektur sistem Smart Door berbasis QR Code [15].

Berdasarkan tinjauan tersebut, terdapat GAP yang jelas yaitu belum adanya penelitian yang mengintegrasikan kriptografi simetri Vigenère dengan steganografi LSB untuk meningkatkan keamanan distribusi kunci pada sistem IoT Smart Door berbasis QR Code. Selain itu, belum banyak penelitian yang mengevaluasi dampak mekanisme keamanan tambahan terhadap kinerja sistem, khususnya delay autentikasi yang sangat penting dalam sistem akses pintu yang mengutamakan kecepatan.

Penelitian ini bertujuan untuk merancang dan mengimplementasikan peningkatan keamanan kunci Vigenère menggunakan steganografi LSB pada sistem IoT Smart Door berbasis QR Code. Pada sistem yang diusulkan, kunci Vigenère disisipkan ke dalam cipherteks menggunakan teknik LSB sehingga distribusi kunci menjadi lebih aman dan tidak mudah terdeteksi. Selanjutnya, penelitian ini mengukur tingkat keamanan terhadap serangan sniffing serta menganalisis pengaruh mekanisme keamanan terhadap delay transmisi data pada jalur komunikasi antara server, website pengguna, ESP-CAM, dan ESP32. Pendekatan ini diharapkan mampu meningkatkan keamanan data, integritas informasi, serta memperkuat perlindungan akses pada sistem Smart Door berbasis IoT.

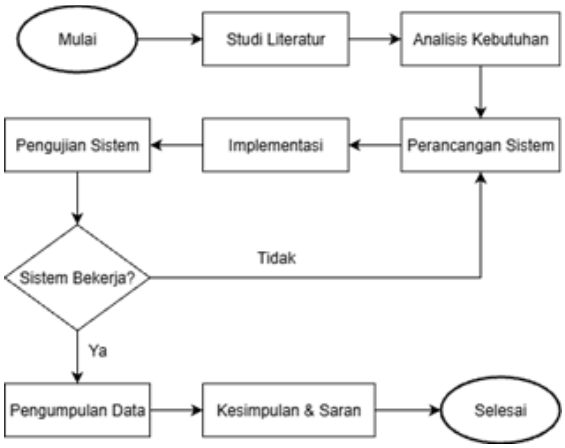
2. METODOLOGI PENELITIAN

Metodologi penelitian ini menjelaskan pendekatan yang digunakan dalam merancang dan menerapkan sistem keamanan komunikasi IoT dengan teknik Steganografi Least Significant Bit (LSB) sebagai media penyembunyian kunci kriptografi. Pendekatan ini bertujuan memastikan proses pengiriman data tidak hanya berjalan secara teknis, tetapi juga mampu menyamarkan kunci enkripsi agar tetap terlindungi selama proses transmisi.

2.1 Tahapan Penelitian

Tahapan penelitian dimulai dengan melakukan studi literatur serta identifikasi kebutuhan sistem, meliputi penggunaan ESP32, ESP32-CAM, Visual Studio Code, Arduino IDE, serta framework Laravel sebagai komponen pengembangan. Tahap berikutnya meliputi perancangan algoritma steganografi LSB untuk penyisipan kunci dan perancangan alur komunikasi data pada tiga jalur sistem IoT. Setelah desain selesai, dilakukan implementasi dan integrasi sistem, kemudian dilanjutkan dengan pengujian melalui sniffing jaringan untuk menilai keberhasilan penyembunyian kunci dan pengujian waktu proses untuk mengevaluasi performa algoritma. Seluruh rangkaian tahapan ini divisualisasikan melalui diagram alir penelitian pada Gambar 1.

Journal of Information System Research (JOSH)
Volume 7, No. 4, Juli 2026, pp 903−913
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i4.9205



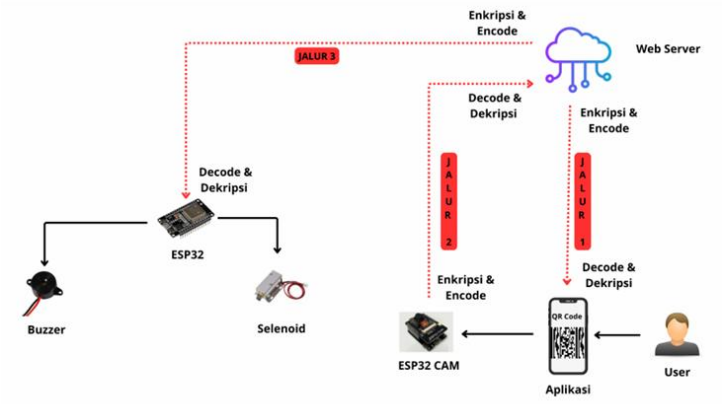
Gambar 1. Tahapan Penelitian

2.1.1 Studi Literatur dan Analisa Kebutuhan

Studi literatur dilakukan untuk memperoleh pemahaman terkait pengembangan sistem Smart Door berbasis IoT, autentikasi menggunakan QR Code, serta pengamanan data menggunakan metode kriptografi Vigenère Cipher dan steganografi Least Significant Bit. Dalam tahap analisis kebutuhan, ditentukan komponen-komponen yang digunakan dalam sistem, yaitu NodeMCU ESP32 sebagai mikrokontroler berbasis Wi-Fi dengan kemampuan pemrosesan yang mendukung aplikasi IoT [16], ESP32-CAM sebagai modul mikrokontroler dengan kamera yang memungkinkan pengambilan gambar secara real-time [17], modul Relay yang berfungsi sebagai saklar elektromagnetik untuk mengontrol beban bertegangan tinggi menggunakan sinyal rendah dari mikrokontroler [18], solenoid door lock sebagai aktuator pengunci pintu elektronik yang bekerja pada tegangan 12V DC [19], serta Buzzer yang digunakan sebagai indikator suara pada sistem [20]. Adapun perangkat lunak yang digunakan meliputi Laravel sebagai framework backend berbasis MVC [21], Arduino IDE untuk pemrograman mikrokontroler [22], Ettercap sebagai alat analisis keamanan jaringan [23], Wireshark untuk menangkap dan menganalisis paket data [24].

2.1.2 Perancangan Sistem

Perancangan sistem dilakukan dengan membangun tiga jalur komunikasi utama antara user, ESP32-CAM, server, dan ESP32, dimana proses pengamanan data dilakukan menggunakan kriptografi Vigenere Cipher untuk mengenkripsi data dan steganografi LSB untuk menyembunyikan kunci di dalam ciphertext sebelum ditransmisikan. Mekanisme ini dirancang agar proses enkripsi, pengiriman data, hingga dekripsi dapat berjalan aman tanpa terlihatnya kunci secara eksplisit. Arsitektur sistem ditunjukkan pada Gambar 2.



Gambar 2. Arsitektur Sistem

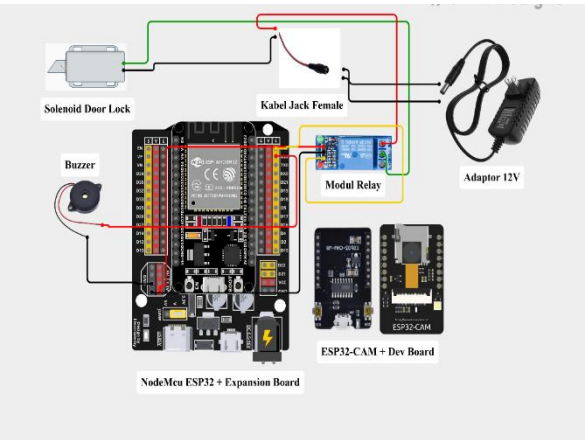
Pada arsitektur tersebut terdapat tiga jalur pengiriman. Jalur pertama menunjukkan proses enkripsi data UUID dilakukan pada server, kemudian kunci disisipkan (encode) dengan metode LSB ke dalam ciphertext dan dikirimkan ke web user. Jalur kedua menunjukkan proses enkripsi data UUID dan Timestamp dilakukan langsung pada perangkat ESP32-CAM, kemudian kunci disisipkan (encode) menggunakan metode LSB, hasilnya dikirimkan ke server, lalu server melakukan ekstraksi kunci (decode) dan dekripsi. Jalur ketiga menunjukkan proses enkripsi data perintah dilakukan pada server, kunci disisipkan (encode) ke ciphertext dengan metode LSB, kemudian dikirimkan ke perangkat ESP32 untuk dilakukan ekstraksi (decode) kunci dan proses dekripsi.

Journal of Information System Research (JOSH)
Volume 7, No. 4, Juli 2026, pp 903−913
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i4.9205

Input pada sistem berupa data UUID dan perintah. Data tersebut diubah menjadi string, kemudian dilakukan enkripsi menggunakan Vigenère Cipher dengan kunci acak. Ciphertext yang dihasilkan kemudian menjadi coverteks untuk proses steganografi. Kunci enkripsi diubah ke bentuk biner, lalu disisipkan ke dalam ciphertext menggunakan metode LSB berbasis teks. Hasil dari proses ini berupa ciphertext yang mengandung kunci tersembunyi. Proses pengiriman data dilakukan dengan mengirimkan dua pesan sekaligus, yaitu ciphertext asli dan ciphertext yang sudah disisipi key. Server kemudian melakukan ekstraksi kunci dari ciphertext yang sudah disisipi key menggunakan metode LSB. Setelah kunci diperoleh, server melakukan dekripsi terhadap ciphertext asli.

2.1.2.1 Perancangan Perangkat Keras

Pada tahap implementasi perangkat keras, seluruh komponen seperti ESP32-CAM, NodeMCU ESP32, Relay, solenoid door lock, dan Buzzer disusun dan dihubungkan sesuai dengan wiring diagram yang ditampilkan pada Gambar 3.



Gambar 3. Skema Perangkat Keras

Gambar 3 merupakan skema perangkat keras yang akan diimplementasikan, seluruh elemen perangkat keras seperti ESP32, ESP32-CAM, Selenoid Door Lock, Relay dan Buzzer akan diterapkan dan dihubungkan. Adapun penggunaan pin ESP32 dengan Relay dan Buzzer dapat dilihat pada Tabel 1.

Tabel 1. Hubungan Pin ESP32 dengan Relay dan Buzzer

ESP32	Komponen
3V	Relay VCC
GND	Relay GND
D23	Relay IN
GND	Buzzer
D22	Buzzer

Adapun penggunaan pin Relay dengan Selenoid Door Lock dan Kabel Jack Female dapat dilihat pada Tabel 2 seperti dibawah ini

Tabel 2. Hubungan Pin Relay dengan Selenoid Door Lock dan Jack Female

Relay	Komponen
COM	Kabel merah selenoid
NO	Kabel merah jack female

2.1.2.2 Algoritma Kriptografi Vigenere Cipher

Vigenère Cipher merupakan algoritma kriptografi simetris yang melindungi pesan teks dengan menggunakan rangkaian sandi Caesar dan pola alfabet yang diterapkan melalui teknik substitusi [8]. Dalam penelitian ini, metode Vigenère Cipher dimodifikasi untuk mengenali 62 karakter yang terdiri atas huruf besar (A–Z), huruf kecil (a–z), dan angka (0–9). Proses enkripsi dilihat pada Persamaan 1.

$$Ci = ((Pi + Ki) \bmod 62) \quad (1)$$

Dari Persamaan 2, ciphertext (C) diperoleh dengan melakukan operasi modulo pada hasil penjumlahan plaintext (P) dan kunci (K). Untuk mendapatkan kembali pesan asli, proses dekripsi dilakukan dengan Persamaan 2.

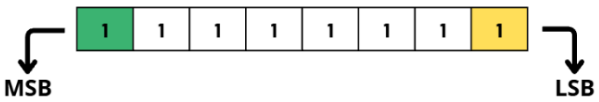
$$Pi = ((Ci - Pi + 62) \bmod 62) \quad (2)$$

Journal of Information System Research (JOSH)
Volume 7, No. 4, Juli 2026, pp 903−913
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i4.9205

Dengan keterangan:
Ci = karakter hasil enkripsi (ciphertext),
Pi = karakter asli (plaintext),
Ki = karakter kunci.

2.1.2.3 Metode Steganografi Least Significant Bit (LSB)

Teknik steganografi Least Significant Bit (LSB) bekerja pada domain spasial dengan melakukan penyisipan data melalui modifikasi bit yang paling tidak signifikan pada sebuah file. Proses ini mudah diterapkan karena perubahan yang dilakukan berada pada tingkat bit paling rendah, sehingga hanya menimbulkan perbedaan yang sangat kecil dan hampir tidak terlihat pada file hasil penyisipan [10]. Ilustrasi posisi LSB dapat dilihat pada Gambar 4.



Gambar 4. Posisi LSB

2.1.3 Implementasi, Pengujian, dan Kesimpulan

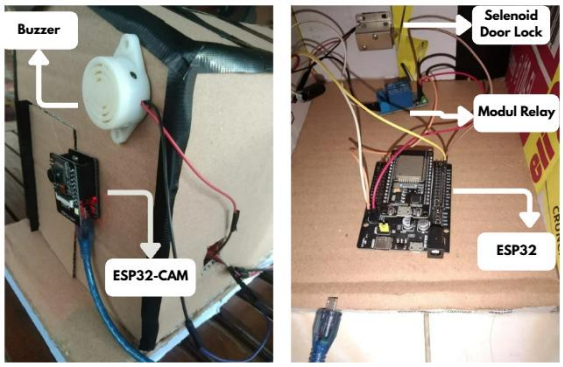
Setelah rancangan selesai dibuat, sistem diimplementasikan pada ESP32, ESP32-CAM, server, dan aplikasi. Pengujian dilakukan dengan mengamati proses enkripsi, penyisipan (encode) kunci dengan Steganografi LSB, pengiriman ciphertext, serta proses ekstraksi (decode) dan dekripsi pada sisi penerima. Selain itu, dilakukan pengukuran waktu proses pada tahap enkripsi dan encode, serta decode dan dekripsi untuk melihat performa algoritma saat dijalankan pada setiap jalur komunikasi. Hasil pengujian kemudian dianalisis untuk menarik kesimpulan terkait keberhasilan penyembunyian kunci dan efisiensi waktu proses, serta menjadi dasar pemberian rekomendasi pengembangan pada penelitian selanjutnya.

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil implementasi dan pengujian pada sistem Smart Door dengan QR Code dilengkapi dengan algoritma kriptografi Vigenere Cipher dan metode steganografi LSB. Pembahasan dimulai dari penerapan perangkat keras dan lunak, dilanjutkan dengan pengujian sniffing perhitungan waktu proses pada tiga jalur komunikasi data yang diterapkan algoritma kriptografi dan steganografi di dalamnya. Seluruh hasil pengujian dianalisis untuk menilai efektivitas sistem dalam menjaga integritas dan keaslian data selama proses transmisi.

3.1 Implementasi Perangkat Keras

Hasil implementasi perangkat keras yang dibuat sesuai dengan skema perangkat keras pada Gambar 3, dapat dilihat pada Gambar 4.



Gambar 4. Implementasi Sistem Smart Door

3.2 Implementasi Perangkat Lunak

Implementasi perangkat lunak menjelaskan bagaimana algoritma kriptografi Vigenere Cipher dan steganografi LSB (Least Significant Bit) diterapkan pada sistem.

3.1.1 Implementasi Kriptografi Vigenere Cipher dan Steganografi LSB

Penerapan kriptografi Vigenere Cipher dan steganografi LSB dilakukan pada tiga jalur komunikasi, yaitu pada jalur Server ke Web User, ESP32-CAM ke Server, dan Server ke ESP32. Pada jalur pertama Server menuju Web User diterapkan enkripsi dan encode untuk mengamankan pengiriman data UUID (Universally Unique Identifier)

Journal of Information System Research (JOSH)
Volume 7, No. 4, Juli 2026, pp 903−913
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i4.9205

yang digunakan sebagai data QR Code tiap user. Pada jalur kedua ESP32-CAM menuju Server, data yang diamankan adalah data hasil pindai QR Code oleh ESP32-CAM yang akan dikirimkan ke Server untuk dilakukan verifikasi. Jalur ketiga Server menuju ESP32, data yang diamankan adalah data hasil verifikasi yang berupa perintah hidupkan selenoid atau nyalakan Buzzer. Selain itu, juga ada proses decode dan dekripsi di tiap destinasi jalur, sehingga dilakukan decode dan dekripsi adalah pada Web User, Server, dan ESP32.
Berikut langkah pada proses enkripsi dan encode, serta proses decode dan dekripsi.
Plainteks : 1cae3d084e854a4c81c159fd5358c32960945962
Kunci : 07o9h

1. Ulangi kunci agar panjangnya sama dengan plainteks. Hasilnya sebagai berikut 07o9h07o9h07o9h07o9h07o9h07o9h07o9h07o9h07o9h
2. Konversi karakter plainteks dan kunci menjadi indeks. Pada penelitian ini digunakan karakter A-Z dengan indeks 0-25, kemudian a-z dengan indeks 26-51, dan 0-9 dengan indeks 52-61. Hasil konversi pada 5 karakter pertama dapat dilihat pada Tabel 3.

Tabel 3. Konversi Karakter Plainteks ke Indeks

No	Plaintext	Pi	Key	Ki
1	1	53	0	52
2	c	28	7	59
3	a	26	o	40
4	e	30	9	61
5	3	55	h	33

3. Lakukan proses enkripsi dengan Persamaan 1. Kemudian konversi indeks ke karakter untuk mendapatkan karakter cipherteks. Hasil proses enkripsi dapat dilihat pada Tabel 4.

Tabel 4. Proses dan Hasil Enkripsi

No	Enkripsi	Cipher Index	Cipher Char
1	(53 + 52) % 62 = 43	43	r
2	(28 + 59) % 62 = 25	25	Z
3	(26 + 40) % 62 = 4	4	E
4	(30 + 61) % 62 = 29	29	d
5	(55 + 33) % 62 = 26	26	a

4. Selanjutnya akan masuk ke proses penyisipan kunci dengan steganografi.
5. Konversi cipherteks dan kunci menjadi bentuk biner. Berikut hasil konversi 5 karakter awal cipherteks dan kunci menjadi biner.

Tabel 5. Konversi ke Biner

Jenis Data	Input	Binary Gabungan
Cipherteks	rZEda	01110010 01011010 01000101 01100100 01100001
Kunci	07o9h	00110000 00110111 01101111 00111001 01101000

6. Proses penyisipan kunci dengan metode steganografi LSB. Langkah pertama adalah pecah cipherteks menjadi per byte (8 bit). Seperti contoh berikut.

Tabel 6. Proses Penyisipan Kunci

Index	Cipher Char	Byte
1	r	1110010
2	Z	1011010
3	E	1000101
4	d	1100100
5	a	1100001

7. Kemudian langkah selanjutnya adalah ambil bit dari kunci, karena disini hanya menggunakan 5 byte, maka bit kunci yang digunakan hanya 5 bit pertama yaitu 0 0 1 1 0.
8. Selanjutnya, lakukan proses LSB dengan mengganti bit terakhir pada tiap byte cipherteks dengan bit kunci. Sehingga didapat hasil sebagai berikut.

Tabel 7. Hasil LSB

Index	Cipher Asli	Hasil Setelah LSB
1	1110010	1110010
2	1011010	1011010
3	1000101	1000101

Journal of Information System Research (JOSH)
Volume 7, No. 4, Juli 2026, pp 903−913
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i4.9205

Index	Cipher Asli	Hasil Setelah LSB
4	1100100	1100101
5	1100001	1100000

Dan hasil perbandingan dapat dilihat pada tabel berikut.

Tabel 8. Perbandingan Bit Sebelum dan Sesudah LSB

Versi	Binary Gabungan
Sebelum LSB	01110010010110100100010101100100011000 01
Setelah LSB	01110010010110100100010101100101011000 00

9. Selanjutnya, biner cipherteks digabung dengan biner hasil LSB beserta kuncinya. Berikut contoh output 5 karakter pertama dari proses tersebut.
   01110010010110100100010101100100011000010111001001011010010001010110010101100000
10. Setelah proses steganografi, data dikonversi agar lebih ringkas sebelum dikirim. Biner hasil diubah menjadi raw bytes, lalu diencode ke Base64. Berikut contoh 6 karakter awal dari hasil konversi akhir.

Tabel 9. Konversi biner ke Base64 Encode

Tahap	Hasil
Input Biner	01110010010110100100010101100100011000010101010 0
Raw Bytes (ASCII)	rZEDaT
Base64 Encode	clpFZGFU

Selanjutnya adalah proses ekstraksi kunci dan dekripsi untuk menghasilkan plainteks.

1. Konversi Base64 Encode ke Raw Bytes dan Biner

Tabel 10. Konversi Base64 Encode ke Biner

Tahap	Hasil
Base64 Encode	clpFZGFU
Raw Bytes (ASCII)	rZEDaT
Biner	01110010010110100100010101100100011000010101010 0

2. Ekstrak kunci dari LSB dilakukan dengan membagi dua biner hasil penerimaan dan mengambil bagian akhir yang berisi cipherteks beserta bit kunci. Biner tersebut dipecah per byte, lalu diambil bit terakhir sebagai kunci. Berikut contoh 5 karakter pertama cipherteks yang memuat kunci.
   01110010 01011010 01000101 01100101 01100000
   Bit kunci adalah 00110
3. Konversi biner cipherteks asli dan biner kunci menjadi ASCII

Tabel 11. Konversi Biner menjadi ASCII

Jenis Data	Data
Biner Cipherteks	01110010010110100100010101100100011000 01
Biner Kunci	00110000001101110110111100111001010110 1000
ASCII Cipherteks	rZEda
ASCII Kunci	07o9h

4. Proses selanjutnya adalah dekripsi. Sama seperti enkripsi, cipherteks dan kunci harus dikonversi ke indeks terlebih dahulu. Berikut hasil konversinya.

Tabel 12. Konversi karakter cipherteks ke indeks

No	Cipher Char	Cipher Index	Key Char	Key Index
1	r	43	0	52
2	Z	25	7	59
3	E	4	o	40
4	d	29	9	61
5	a	26	h	33

5. Langkah selanjutnya lakukan proses dekripsi dengan Persamaan 2. Setelah didapat hasil perhitungan persamaan dekripsi, selanjutnya ubah bentuk indeks menjadi karakter.

Tabel 13. Proses Dekripsi

No	(C - K + 62) mod 62	Plain Index	Plain Char
1	(43 - 52 + 62) mod 62 = 53	53	1

Journal of Information System Research (JOSH)
Volume 7, No. 4, Juli 2026, pp 903−913
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i4.9205

No	(C - K + 62) mod 62	Plain Index	Plain Char
2	(25 - 59 + 62) mod 62 = 28	28	c
3	(4 - 40 + 62) mod 62 = 26	26	a
4	(29 - 61 + 62) mod 62 = 30	30	e
5	(26 - 33 + 62) mod 62 = 55	55	3

Maka didapat hasil dekripsi berupa plainteks sebagai berikut.
1cae3d084e854a4c81c159fd5358c32960945962

3.3 Pengujian Sniffing

Pengujian sniffing dilakukan pada tiga jalur komunikasi data yang telah menerapkan kriptografi Vigenère Cipher dan steganografi LSB. Tujuan pengujian ini adalah memastikan bahwa data yang dikirim pada setiap jalur benar-benar telah melalui proses enkripsi dan penyisipan, dengan cara membandingkan hasil tangkapan sniffing dengan data sebelum dilakukan enkripsi dan encode. Pengujian dilakukan dengan menyimulasikan serangan sniffing menggunakan Ettercap, kemudian menangkap lalu lintas data menggunakan Wireshark. Data yang berhasil ditangkap selanjutnya disusun dalam bentuk tabel sesuai dengan jalur komunikasi yang diuji.

Tabel 14. Pengujian Keamanan untuk Pengiriman Data Autentikasi

Percobaan	Data Autentikasi (UUID)	Data Hasil Sniffing
1	1cae3d084e84a4c81c159fd5358c329	WVdYRGFYeGhiWTVlYlUxQmZ2WmFjM2NDY3gyaDl4emlYV1lEYVh4aGJYNWViVTBCZnZbYWIzY0NieTNoOXh7aA==
2	1cae3d084e84a4c81c159fd5358c329	ZTJSeGczclJoNHpPaDB2dmxSVEtpWld3aVR3UkZUdFNkM1N4ZzNzUmg1e05oMHZ3bFJVS2haVndoVXZTRlV0Ug==
…	…	…
30	b59dd7ef9159406f8bb6bad6cefad66b	V09Fa1lRam00S0FHekpCbTN1Z0RXdGlEWHhraFlQQmlWTkVrWFFqbTRLQEd6S0JsMnVmRFZ1aURYeWpoWVBCaA==

Data pada Tabel 14 menunjukkan hasil sniffing pada jalur pertama, yaitu pengiriman UUID dari server ke website pengguna. Pengujian dilakukan 30 kali menggunakan 6 QR Code berbeda. Setiap tangkapan menghasilkan 88 karakter data hasil encode, sedangkan plainteks UUID berisi 32 karakter. Seluruh hasil sniffing selalu berbeda dari plainteks, bahkan untuk UUID yang sama, sehingga menandakan penggunaan kunci dinamis serta keberhasilan penerapan kriptografi dan steganografi.

Tabel 15. Pengujian Keamanan untuk Pengiriman data QR Code

Percobaan	Data Pembacaan QR Code	Data Hasil Sniffing
1	1cae3d084e854a4c81c159fd5358c32960945962	clpFZGFUeG0zQnkyaVpiUzVmYll2NkpjY3QybWJhczZremd1Mm41WnJaRWVgVHhsMkJ5M2hbY1M0Z2NYdzdLY2J0M21jYHI3antndDNuNFo=
2	1cae3d084e854a4c81c159fd5358c32960177731	bjBpVklQT0d2dHVUQ1JKT1c5VEdyWG5VS3BUR1RJb1hFckd0VkZ1R24xaVdIUU9HdnV0VUNSSk9WOVRGc1huVUpwVUdUSG5ZRHNGdVZGdEY=
…	…	…
30	b59dd7ef9159406f8bb6bad6cefad66b60180068	OFI1cTZlMGJNVWNWMERaQ1VYb1o4d1pKNUIxV3FaZHgyRFVmTXdKYjhTNXA3ZDBiTFViVzBFW0NUWG9bOHdbSjRDMFZxW2V4MkVVZkx3SmI=

Data pada tabel menampilkan hasil sniffing pada jalur kedua, yaitu pengiriman UUID dari ESP32-CAM ke server. Pengujian dilakukan 30 kali menggunakan 6 QR Code berbeda. Setiap tangkapan berisi 108 karakter hasil encode, sedangkan plainteks terdiri dari 40 karakter (32 UUID dan 8 timestamp). Seluruh hasil sniffing selalu berbeda dari plainteks, termasuk untuk data yang sama, sehingga menunjukkan kunci bersifat dinamis dan penerapan kriptografi serta steganografi berjalan dengan baik.

Tabel 16. Pengujian Keamanan untuk Pengiriman Intruksi

Percobaan	Data Perintah	Data Hasil Sniffing
1	Unlock	ZjhaTE41Z0JXemJMVHlpS2VGWThmNU9NVDhoUllKTzdmOVtNTjVnQlZ7Yk1UeWlKZEdZOWc0Tk1UOWlSWUpONg==

Journal of Information System Research (JOSH)
Volume 7, No. 4, Juli 2026, pp 903−913
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i4.9205

Percobaan	Data Perintah	Data Hasil Sniffing
2	Unlock	YXlGWEl2TU5ScEhYT29PV1o1RUthdjRZT3lOZFQ5NEpgeUdZSHZMT1JxSFhPb05WWjVFSmB3NFlOeU9lVDk0Sg==
…	…	…
30	Buzzer	d3hpams0VlZrNldmOUlaYzQ2b2Z1Q2pXazNWVjJ4bmR2eWhqazRXV2o3Vmc4SVpiNDZvZ3RDaldqM1dXMnlvZA==

Data pada tabel menunjukkan hasil sniffing pada jalur ketiga, yaitu pengiriman perintah unlock dan Buzzer ke ESP32. Pengujian dilakukan 30 kali, masing-masing 15 kali untuk setiap perintah. Seluruh hasil sniffing selalu berbeda dari plainteks, bahkan untuk perintah yang sama, sehingga menandakan kunci bersifat dinamis dan penerapan kriptografi serta steganografi berhasil.

3.4 Pengujian Waktu Proses

Pengujian ini bertujuan untuk mengukur durasi waktu enkripsi dan encode serta dekripsi dan decode pada setiap tahap komunikasi dalam sistem untuk melihat seberapa lama algoritma Vigenere Chiper dan Penambahan Steganografi LSB dalam menangani data dalam sistem. Pengujian dilakukan pada tiga jalur komunikasi utama, yaitu pengukuran waktu enkripsi dan dekripsi pada server, ESP32-CAM, dan website pengguna.

Tabel 17. Pengujian Waktu Enkripsi dan Encode Data Autentikasi

Percobaan	Waktu Enkripsi dan Encode di Server (ms)	Waktu Decode dan Dekripsi di Web User (ms)
1	0,13	0,11
2	0,17	0,19
…	…	…
15	0,11	0,18
Rata-rata	0,14	0,13

Tabel 17 menunjukkan waktu enkripsi dan encode pada server sebagai durasi proses pengamanan UUID menggunakan Vigenère dan steganografi LSB, serta waktu dekripsi dan decode pada web user untuk membuka kembali ciphertext menjadi QR Code. Dari 15 percobaan, rata-rata waktu enkripsi tercatat 0,14 ms dan waktu dekripsi 0,13 ms.

Tabel 18. Pengujian Waktu Enkripsi dan Encode Data Pembacaan QR Code

Percobaan	Waktu Enkripsi dan Encode di ESP32-CAM (ms)	Waktu Decode dan Dekripsi di Server (ms)
1	2,21	0,08
2	2,22	0,08
…	…	…
15	2,22	0,08
Rata-rata	2,22	0,1

Tabel 18 menunjukkan waktu enkripsi dan encode pada ESP32-CAM sebagai durasi proses pengamanan data hasil pembacaan QR Code menggunakan Vigenère dan steganografi LSB sebelum dikirim ke Server, serta waktu dekripsi dan decode pada server untuk membuka kembali data tersebut. Dari 15 percobaan, rata-rata waktu enkripsi adalah 2,22 ms dan waktu dekripsi 0,10 ms.

Tabel 19. Pengujian Waktu Enkripsi dan Encode Data Autentikasi

Percobaan	Waktu Enkripsi dan Encode di Server (ms)	Waktu Decode dan Dekripsi di ESP32 (ms)
1	0,17	1,46
2	0,1	1,46
…	…	…
15	0,09	1,47
Rata-rata	0,1	1,46

Tabel 19 menampilkan waktu enkripsi dan encode pada server sebagai durasi pengamanan data instruksi menggunakan Vigenère dan steganografi LSB sebelum dikirim ke ESP32, serta waktu dekripsi dan decode pada ESP32 untuk membuka kembali data tersebut. Dari 15 percobaan, rata-rata waktu enkripsi sebesar 0,10 ms dan waktu dekripsi 1,46 ms.

Journal of Information System Research (JOSH)
Volume 7, No. 4, Juli 2026, pp 903−913
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i4.9205

3.5 Pembahasan

Penelitian ini berhasil mengimplementasikan kombinasi kriptografi Vigenère Cipher dan steganografi LSB untuk meningkatkan keamanan komunikasi pada sistem Smart Door berbasis IoT. Hasil pengujian sniffing pada tiga jalur komunikasi menunjukkan bahwa seluruh data yang tertangkap selalu berupa ciphertext Base64 dan tidak pernah menampilkan plainteks, bahkan ketika data aslinya sama. Hal ini membuktikan bahwa penggunaan kunci dinamis dan penyisipan melalui LSB efektif dalam mencegah penyadapan. Pengujian waktu proses juga menunjukkan bahwa kombinasi kedua metode dapat diimplementasikan secara efisien pada perangkat dengan sumber daya terbatas. ESP32-CAM menghasilkan waktu enkripsi dan encode rata-rata 2,22 ms, sedangkan server dan web user memiliki waktu proses yang lebih singkat. Waktu decode dan dekripsi 1,46 ms pada ESP32 masih dalam batas wajar untuk sistem IoT. Teknik LSB turut menjaga keamanan dengan menyembunyikan kunci dalam ciphertext tanpa mengubah karakteristik data secara signifikan. Secara keseluruhan, gabungan Vigenère Cipher dan steganografi LSB terbukti meningkatkan keamanan sistem tanpa menambah beban proses secara signifikan, sehingga cocok untuk aplikasi Smart Door yang membutuhkan komunikasi data yang aman dan tetap responsif.

4. KESIMPULAN

Berdasarkan hasil penelitian, mekanisme pengamanan yang diterapkan mampu melindungi data komunikasi dari potensi penyadapan, yang ditunjukkan oleh seluruh data yang ditransmisikan berubah menjadi ciphertext pada setiap jalur komunikasi yang diuji. Dari sisi kinerja, waktu rata-rata proses enkripsi dan encode di server sebesar 0,14 ms, sedangkan untuk proses decode dan dekripsi di web pengguna membutuhkan waktu rata-rata 0,13 ms. Pada perangkat ESP32-CAM, rata-rata waktu enkripsi dan encode tercatat sebesar 2,22 ms, sedangkan untuk proses decode dan dekripsi di server 0,10 ms. Sementara itu pada perangkat ESP32 rata-rata waktu enkripsi dan encode di server sebesar 0,10 ms, sedangkan untuk proses decode dan dekripsi di perangkat ESP32 sebesar 1,46 ms. Hasil tersebut menunjukkan bahwa penambahan mekanisme pengamanan tidak memberikan beban signifikan terhadap performa sistem, sehingga pendekatan yang digunakan efektif dalam menjaga keamanan komunikasi data dengan tetap mempertahankan efisiensi proses.

REFERENCES

[1] M. S. Nasution, M. Amin, and W. Fitriani, “Smart sistem IoT pemberi pakan ikan dengan menggunakan metode time scheduling berbasis mikrokontroller,” J. Zetroem, vol. 05, no. 02, pp. 161–164, 2023.
[2] M. A. Juniawan and A. H. Rismayana, “Prototipe smart door lock berbasis internet of things (studi kasus lab komputer Politeknik TEDC Bandung),” JATI, vol. 8, no. 5, pp. 10856–10861, 2024.
[3] A. Rabbani, “Sistem informasi reservasi dan pembayaran resto berbasis QR code,” Electrician, vol. 17, no. 1, pp. 77–82, 2023, doi: 10.23960/elc.v17n1.2423.
[4] E. Lantz and T. Pierrou, “Security evaluation of a smart door lock system,” KTH Royal Institute of Technology, 2022.
[5] H. Fereidouni, O. Fadeitcheva, and M. Zalai, “IoT and man-in-the-middle attacks,” Secur. Priv., vol. 8, no. e70016, pp. 1–9, 2025, doi: 10.1002/spy2.70016.
[6] A. Tamsir, I. Irwansyah, and M. S. Huda Mubarok, “Analisis keamanan jaringan WiFi mahasiswa UBD dari serangan packet sniffing,” JIF, vol. 12, no. 01, pp. 53–58, 2024, doi: 10.33884/jif.v12i01.8739.
[7] P. Simamora and S. A. Pasaribu, “Kunci simetris pada perangkat IoT: Kajian literatur,” SISFOTEKJAR, vol. 5, no. 2, pp. 49–55, 2024.
[8] M. Rivaldi, I. Z. Harahap, H. Isdianto, and R. A. Putri, “Implementasi algoritma kriptografi Vigenere Cipher pada pengamanan pesan text berbasis web,” Positif J. Sist. dan Teknol. Inf., vol. 9, no. 1, pp. 57–61, 2023, doi: 10.31961/positif.v9i1.1611.
[9] D. M. Sekab et al., “Pengamanan teks SMS melalui pendekatan multiple encryption menggunakan algoritma RSA dan 3DES,” LintekEdu, vol. 6, no. 2, pp. 398–408, 2025.
[10] A. R. Mido and I. H. U. Ujianto, “Analisis pengaruh citra terhadap kombinasi kriptografi RSA dan steganografi LSB,” JTIIK, vol. 9, no. 2, pp. 279–286, 2022, doi: 10.25126/jtiik.202294852.
[11] A. Basit, A. Sya’bani Putra, G. Ayu Revira, and R. Nur Widia, “Smart door lock berbasis QR code,” Smart Comp, vol. 11, no. 1, pp. 5–8, 2022, doi: 10.30591/smartcomp.v11i1.3179.
[12] I. Murni, A. S. Br pa, B. R. Lubis, and A. Ikhwan, “Pengamanan pesan rahasia dengan algoritma Vigenere Cipher menggunakan PHP,” J. Educ., vol. 5, no. 2, pp. 3466–3476, 2023, doi: 10.31004/joe.v5i2.1027.
[13] E. H. Rachmawanto, R. S. Gumelar, Q. Nabila, C. A. Sari, and R. R. Ali, “Testing data security using a vigenere cipher based on the QR code,” Kinetik, vol. 4, no. 4, pp. 701–708, 2023.
[14] C. Umam et al., “Kombinasi steganografi LSB dan kriptografi AES dalam sekuriti teks rahasia pada citra berwarna,” SEMNASTEKMU, vol. 2, no. 1, pp. 109–118, 2022.
[15] R. P. Harahap and A. H. Hasugian, “Teknik keamanan data menggunakan metode Vigenere Cipher dan steganografi dalam penyisipan pesan teks pada citra,” J. Fasilkom, vol. 13, no. 3, pp. 570–577, 2023.
[16] H. A. Wahid, J. Maulindar, and A. I. Pradana, “Rancang bangun sistem penyiraman tanaman otomatis aglonema berbasis IoT menggunakan Blynk dan NodeMCU 32,” INNOVATIVE, vol. 3, no. 2, pp. 6265–6276, 2023.
[17] D. Setiawan, H. Jaya, S. Nurarif, T. Syahputra, and M. Syahril, “Implementasi ESP32-CAM dan Blynk pada WiFi door lock system menggunakan teknik duplex,” J. Sci. Soc. Res., vol. 5, no. 1, p. 159, 2022, doi: 10.54314/jssr.v5i1.807.
[18] R. Juliansyah, E. Fitriani, N. Paramita, and A. Ariyadi, “Rancang bangun sistem kontrol motor feeder dan monitoring pakan ikan nila berbasis Smart Relay Zelio,” J. Pendidik. Tambusai, vol. 8, pp. 11157–11167, 2024.

Journal of Information System Research (JOSH)
Volume 7, No. 4, Juli 2026, pp 903−913
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i4.9205

[19] Z. Avista and O. Fahlovi, "Rancang bangun smart door access berbasis fingerprint untuk keamanan ruang laboratorium," Venus J. Publ. Rumpun Ilmu Tek., vol. 2, no. 1, pp. 1–13, 2024.
[20] I. A. Deswiyan, S. Solikhun, S. Sumarno, P. Poningsih, and S. R. Andani, "Rancang Bangun Alat Pendeteksi Ketinggian Air dan Alarm Pemberitahuan Antisipasi Datangnya Banjir Berbasis Arduino Uno," J. Penelit. Inov., vol. 1, no. 2, pp. 155–164, 2021, doi: 10.54082/jupin.23.
[21] W. Muthia Kansha, Saherih, and Muchlis, "Rancang bangun alat pendeteksi ketinggian air dan alarm pemberitahuan antisipasi datangnya banjir berbasis Arduino Uno," J. Tek. Inform. STMIK Antar Bangsa, vol. 9, no. 1, pp. 25–31, 2023.
[22] A. Herlan, I. Fitri, and R. Nuraini, "Rancang bangun sistem monitoring data sebaran Covid-19 secara real-time menggunakan Arduino berbasis internet of things (IoT)," J. JTIK (Jurnal Teknol. Inf. dan Komunikasi), vol. 5, no. 2, p. 206, 2021, doi: 10.35870/jtik.v5i2.212.
[23] N. Santi and Y. Mulyanto, "Analisis kelayakan jaringan komputer menggunakan alat sniffing dan intrusion detection system (IDS)," JATI, vol. 8, no. 4, pp. 6141–6147, 2024, doi: 10.36040/jati.v8i4.10079.
[24] M. A. Rizkiawan, E. Kurniawan, and H. Ramza, "Analisis quality of service jaringan nirkabel menggunakan Wireshark dengan metode action research," JATI, vol. 8, no. 5, pp. 9876–9882, 2024.