Scripta Technica:
Journal of Engineering and Applied Technology
Vol 1 No 2 Desember 2025, Hal. 386-399
ISSN:3110-0775(Print) ISSN: 3109-9696(Electronic)
Open Access: https://scriptaintelektual.com/scripta-technica

Perancangan Sistem Monitoring Keamanan Brankas Rumah Berbasis Internet of Things (IoT) secara Real-Time melalui Telegram Bot

Yesaya IXVois Hendrikus Sereh[1*], Mizanul Achlaq[2], Agung Widodo[3]
[1-3] Universitas Narotama, Indonesia
email: voissereh12@gmail.com[1]

Article Info :
Received:
25-11-2025
Revised:
20-12-2025
Accepted:
31-12-2025

Abstract

This study presents the design and development of a real-time IoT-based monitoring security system for home safes integrated with Telegram Bot notifications. The proposed system employs NodeMCU ESP8266 as the main controller, combined with an HC-SR04 ultrasonic sensor for motion detection and an MPU-6500 vibration sensor for shock recognition. When suspicious movement or abnormal vibration is detected, the system activates a local buzzer alarm and triggers an automatic solenoid door lock mechanism through a relay module. Simultaneously, warning messages are transmitted instantly to users via Telegram Bot and displayed on a web-based monitoring dashboard. Experimental evaluation indicates that the ultrasonic sensor achieved an average measurement error of ±1.6 cm, while vibration detection responded within 0.2–0.5 seconds. The solenoid locking mechanism demonstrated 100% success across all test scenarios. Telegram notifications were delivered with an average latency of 1.33 seconds, depending on network quality. The optimization stage improved detection stability, reduced false alarms, and enhanced system reliability. Overall, the developed prototype offers an effective and low-cost smart security solution for domestic safe protection.

***Keywords**: IoT security system, home safe monitoring, Telegram Bot notification, NodeMCU ESP8266, smart lock automation.*

Abstrak

Penelitian ini memaparkan desain dan pengembangan sistem pemantauan keamanan berbasis IoT real-time untuk brankas rumah yang terintegrasi dengan notifikasi Telegram Bot. Sistem yang diusulkan menggunakan NodeMCU ESP8266 sebagai pengontrol utama, dikombinasikan dengan sensor ultrasonik HC-SR04 untuk deteksi gerakan dan sensor getaran MPU-6500 untuk pengenalan guncangan. Ketika gerakan mencurigakan atau getaran abnormal terdeteksi, sistem mengaktifkan alarm buzzer lokal dan memicu mekanisme penguncian pintu solenoid otomatis melalui modul relay. Secara bersamaan, pesan peringatan dikirimkan secara instan kepada pengguna melalui Telegram Bot dan ditampilkan pada dashboard pemantauan berbasis web. Evaluasi eksperimental menunjukkan bahwa sensor ultrasonik mencapai kesalahan pengukuran rata-rata ±1,6 cm, sementara deteksi getaran merespons dalam waktu 0,2–0,5 detik. Mekanisme penguncian solenoid menunjukkan keberhasilan 100% di semua skenario uji. Pemberitahuan Telegram dikirim dengan latensi rata-rata 1,33 detik, tergantung pada kualitas jaringan. Tahap optimasi meningkatkan stabilitas deteksi, mengurangi alarm palsu, dan meningkatkan keandalan sistem. Secara keseluruhan, prototipe yang dikembangkan menawarkan solusi keamanan pintar yang efektif dan berbiaya rendah untuk perlindungan brankas domestik.

Kata kunci: Sistem keamanan IoT, pemantauan keamanan rumah, pemberitahuan melalui Telegram Bot, NodeMCU ESP8266, otomatisasi kunci pintar.

PENDAHULUAN

Perkembangan Internet of Things (IoT) dalam satu dekade terakhir telah mentransformasi paradigma keamanan domestik dari sistem statis berbasis perangkat lokal menjadi ekosistem cerdas yang terhubung secara global, di mana perangkat sensor, modul komunikasi, dan platform notifikasi real-time berinteraksi untuk menghasilkan respons keamanan yang adaptif dan berkelanjutan. Dalam konteks meningkatnya urbanisasi, mobilitas masyarakat, serta kompleksitas ancaman kriminalitas rumah tangga, kebutuhan terhadap sistem pengamanan rumah yang mampu melakukan monitoring jarak jauh secara instan menjadi semakin mendesak, terutama ketika objek yang diamankan memiliki nilai tinggi seperti brankas rumah. Integrasi aplikasi pesan instan seperti Telegram dalam arsitektur IoT muncul sebagai pendekatan mutakhir karena menawarkan jalur komunikasi cepat, fleksibel, dan relatif

murah dibandingkan infrastruktur keamanan konvensional, sekaligus memungkinkan automasi berbasis bot yang dapat mempercepat pengambilan keputusan pengguna dalam situasi darurat (Suthar & Patel, 2025; Wahyudi et al., 2025).

Literatur internasional menunjukkan bahwa implementasi Telegram Bot dalam sistem keamanan rumah telah berkembang pesat dengan fokus pada peningkatan aksesibilitas dan efektivitas monitoring berbasis IoT. Sejumlah studi menegaskan bahwa Telegram mampu berfungsi sebagai antarmuka kontrol dan notifikasi yang responsif dalam sistem keamanan rumah, baik untuk mendeteksi intrusi maupun memantau perangkat secara jarak jauh. Fadhlurrohman dan Basri (2025) memperlihatkan bahwa Telegram Bot dapat dimanfaatkan untuk mengurangi keterlambatan komunikasi dalam sistem anti-pencurian berbasis IoT, sementara Jibin et al. (2025) mengembangkan sistem pengawasan berbasis ESP32-CAM yang memanfaatkan Telegram sebagai media pengiriman citra secara real-time. Rambabu et al. (2025) juga menekankan pentingnya integrasi motion detection dengan notifikasi instan sebagai mekanisme mitigasi ancaman, yang memperlihatkan bahwa tren riset bergerak menuju sistem keamanan rumah yang semakin otonom dan responsif terhadap perubahan lingkungan.

Meskipun demikian, sintesis kritis atas penelitian terdahulu mengindikasikan bahwa sebagian besar pengembangan IoT–Telegram masih berorientasi pada keamanan rumah secara umum, belum secara spesifik menargetkan objek dengan kebutuhan proteksi tinggi seperti brankas rumah yang memerlukan tingkat monitoring lebih ketat dan mekanisme respons lebih terstruktur. Studi Afiyat et al. (2026), misalnya, menyoroti efektivitas Telegram Bot dalam sistem deteksi kebocoran gas rumah tangga, menunjukkan bahwa pendekatan notifikasi real-time sangat relevan dalam konteks keselamatan, namun desainnya berbeda secara konseptual dengan sistem keamanan fisik terhadap ancaman pencurian. Penelitian Putra et al. (2025) pada integrasi RFID dan Telegram Bot dalam sistem akses pintu otomatis memperlihatkan potensi kontrol berbasis identifikasi, tetapi fokusnya masih pada manajemen akses, bukan pada monitoring keamanan brankas yang membutuhkan kombinasi sensor intrusi, alarm, serta pelaporan kondisi secara kontinu.

Celah konseptual dan empiris dalam literatur menjadi semakin jelas ketika dicermati bahwa banyak sistem yang telah dikembangkan belum sepenuhnya mengatasi tantangan reliabilitas monitoring real-time, terutama dalam skenario keamanan objek spesifik dengan risiko tinggi. Beberapa penelitian menitikberatkan pada aspek prototipe tanpa evaluasi komprehensif terhadap ketahanan sistem terhadap gangguan jaringan atau false alarm, sementara studi lain lebih menonjolkan integrasi perangkat keras tanpa mengembangkan kerangka monitoring yang sistematis untuk mendukung keputusan pengguna secara cepat. Oyon et al. (2025) memang menunjukkan optimasi automasi berbasis Telegram Bot untuk kontrol perangkat jarak jauh, tetapi pendekatan tersebut belum menjawab kebutuhan pengamanan brankas yang mensyaratkan deteksi ancaman berbasis multi-sensor dan notifikasi berlapis. Ketidakkonsistenan ini menegaskan bahwa masih terdapat ruang penelitian untuk merancang sistem monitoring keamanan yang lebih terfokus, robust, dan kontekstual terhadap kebutuhan pengamanan brankas rumah (Suthar & Patel, 2025; Rambabu et al., 2025).

Urgensi ilmiah dan praktis dari persoalan ini terletak pada meningkatnya kebutuhan sistem keamanan domestik yang tidak hanya reaktif, tetapi juga preventif dan mampu menyediakan informasi real-time yang akurat bagi pengguna. Dalam ekosistem smart home dan smart city, keamanan rumah tidak dapat dipisahkan dari infrastruktur digital yang lebih luas, sehingga sistem monitoring brankas berbasis IoT berpotensi menjadi komponen penting dalam manajemen keamanan urban yang terintegrasi. Wahyudi et al. (2025) menegaskan bahwa sistem keamanan IoT yang mendukung smart city harus mampu memberikan monitoring dan manajemen yang adaptif, sedangkan penelitian Jibin et al. (2025) dan Fadhlurrohman dan Basri (2025) menguatkan bahwa Telegram Bot menawarkan jalur komunikasi instan yang efektif. Namun, belum adanya rancangan spesifik untuk pengamanan brankas rumah menunjukkan adanya kebutuhan mendesak untuk mengisi gap ini, baik dalam ranah akademik maupun implementasi nyata.

Penelitian ini menempatkan diri dalam lanskap keilmuan IoT security dengan fokus pada perancangan sistem monitoring keamanan brankas rumah berbasis Internet of Things yang mampu bekerja secara real-time melalui integrasi Telegram Bot sebagai media notifikasi dan kontrol jarak jauh. Studi ini bertujuan untuk mengembangkan pendekatan yang lebih spesifik dan terstruktur dibandingkan penelitian sebelumnya dengan menggabungkan konsep deteksi intrusi, monitoring kondisi brankas, serta sistem komunikasi instan yang dapat meningkatkan respons pengguna terhadap potensi ancaman. Kontribusi utama penelitian ini tidak hanya terletak pada aspek implementasi teknis, tetapi juga pada

penguatan kerangka metodologis dalam desain sistem keamanan objek bernilai tinggi, sehingga diharapkan dapat memperkaya diskursus teoretis tentang smart security monitoring sekaligus memberikan solusi praktis yang relevan untuk kebutuhan keamanan domestik modern.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan Research and Development (R&D) yang berorientasi pada perancangan, pembangunan, serta pengujian prototipe sistem monitoring keamanan brankas rumah berbasis Internet of Things (IoT) secara real-time melalui integrasi Telegram Bot. Pendekatan ini dipilih karena penelitian tidak berhenti pada kajian konseptual, melainkan menghasilkan produk teknologi yang dapat dioperasikan dan dievaluasi langsung dalam konteks keamanan domestik. Proses pengembangan sistem mengikuti model PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) yang menyediakan tahapan sistematis mulai dari identifikasi kebutuhan dan studi literatur pada fase prepare, perencanaan komponen perangkat keras dan perangkat lunak pada fase plan, hingga perancangan arsitektur sistem serta logika komunikasi sensor–mikrokontroler–aktuator pada fase design. Implementasi dilakukan melalui integrasi NodeMCU ESP8266 sebagai pusat kendali, sensor ultrasonik HC-SR04 untuk deteksi pergerakan, sensor MPU-6500 untuk membaca getaran atau guncangan, buzzer sebagai alarm lokal, serta solenoid door lock sebagai mekanisme penguncian otomatis, sementara Telegram Bot berperan sebagai kanal notifikasi instan dan antarmuka kontrol jarak jauh.

Pengumpulan data dilakukan melalui kombinasi studi pustaka, observasi, eksperimen, dan dokumentasi untuk memastikan sistem diuji secara komprehensif dalam berbagai skenario ancaman. Tahap operate difokuskan pada pengujian fungsional sistem dalam kondisi nyata, termasuk evaluasi respons sensor terhadap aktivitas mencurigakan, aktivasi buzzer dan penguncian otomatis, serta keberhasilan pengiriman notifikasi real-time melalui Telegram. Tahap optimize kemudian dilakukan berdasarkan hasil evaluasi operasional dengan penyesuaian parameter sensor, konfigurasi program, serta peningkatan stabilitas konektivitas agar sistem bekerja lebih andal. Analisis data dilakukan secara deskriptif dengan dukungan pengukuran kuantitatif sederhana, seperti waktu respons, akurasi deteksi, dan kecepatan notifikasi, sehingga efektivitas sistem dapat dinilai berdasarkan kesesuaian performa aktual dengan kriteria keberhasilan yang telah ditetapkan dalam rancangan penelitian.

HASIL DAN PEMBAHASAN

Tahap Prepare dan Plan sebagai Fondasi Konseptual Sistem Monitoring Keamanan Brankas Berbasis IoT

Tahap prepare dalam pengembangan sistem monitoring keamanan brankas berbasis IoT bukan sekadar tahap awal administratif, melainkan menjadi fondasi epistemik yang menentukan arah konseptual seluruh rancangan keamanan digital yang akan dibangun, terutama ketika objek yang diamankan adalah brankas rumah yang memiliki karakter risiko tinggi dan kebutuhan proteksi lebih ketat dibanding sistem smart home umum. Literatur keamanan IoT modern menegaskan bahwa ancaman domestik tidak lagi hanya bersifat fisik, tetapi juga terkait keterbatasan monitoring real-time yang menyebabkan keterlambatan respons pengguna ketika terjadi intrusi atau manipulasi perangkat (Wahyudi et al., 2025). Dalam konteks ini, pemetaan kebutuhan sistem seperti deteksi pergerakan, deteksi getaran, alarm lokal, penguncian otomatis, serta notifikasi instan melalui Telegram menunjukkan bahwa penelitian ini bergerak pada paradigma keamanan adaptif berbasis multisensor. Kerangka tersebut sejalan dengan tren sistem keamanan rumah berbasis notifikasi mobile yang menekankan pentingnya komunikasi instan sebagai mekanisme mitigasi risiko (Medina-Ángel & Burlak, 2025). Dengan demikian, prepare menjadi tahap kritis untuk menghubungkan kebutuhan praktis dengan kerangka teoritik IoT security yang berkembang dalam literatur internasional.

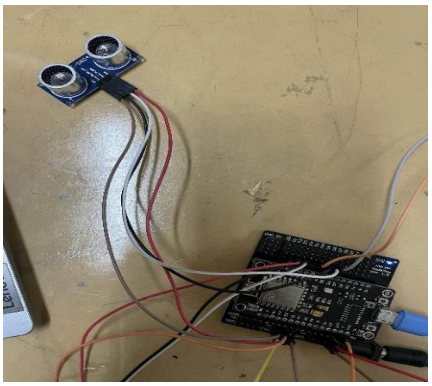
Secara konseptual, identifikasi masalah pada tahap prepare memperlihatkan bahwa sistem pengamanan brankas konvensional yang masih manual menghadapi keterbatasan mendasar karena tidak memiliki kemampuan sensing dan komunikasi jarak jauh, sehingga potensi ancaman sering terdeteksi setelah kejadian berlangsung. Studi Suthar dan Patel (2025) menegaskan bahwa integrasi Telegram dalam IoT home security dapat mempercepat penyampaian informasi ancaman dibanding sistem berbasis alarm lokal semata, karena pengguna dapat segera menerima peringatan melalui perangkat mobile. Namun, penelitian terdahulu lebih banyak menempatkan keamanan rumah sebagai ruang terbuka (door security, surveillance umum), bukan objek tertutup seperti brankas yang memerlukan

parameter monitoring berbeda. Hal ini menunjukkan adanya kebutuhan konseptual untuk membangun sistem yang tidak hanya mendeteksi intrusi eksternal, tetapi juga mendeteksi manipulasi fisik seperti getaran atau hentakan yang mengindikasikan upaya pembobolan (Nannung & Miru, 2025). Tahap prepare dalam penelitian ini menjadi respons langsung terhadap gap tersebut dengan merumuskan kebutuhan keamanan berbasis sensor jarak dan sensor inersia secara simultan.

Tahap plan kemudian berfungsi sebagai proses translasi kebutuhan konseptual ke dalam arsitektur teknis, di mana pemilihan NodeMCU ESP8266 sebagai pusat kendali menunjukkan orientasi pada solusi low-cost namun tetap memiliki konektivitas Wi-Fi yang stabil untuk mendukung komunikasi real-time. Pilihan ini sejalan dengan berbagai studi yang menekankan efektivitas mikrokontroler ESP-series dalam sistem monitoring keamanan berbasis Telegram, baik untuk deteksi gerak maupun kontrol jarak jauh (Antono & Suryo, 2025; Putra F. P. et al., 2025). Integrasi sensor ultrasonik HC-SR04 dan sensor getar MPU-6500 juga memperlihatkan pendekatan multisensor yang dianggap lebih reliabel dalam meminimalkan false alarm dibanding sistem single-sensor. Konsep adaptive monitoring semacam ini juga ditekankan dalam studi hazard detection IoT yang menuntut sistem mampu menyesuaikan sensitivitas berdasarkan kondisi lingkungan (Kok et al., 2025). Dengan demikian, tahap plan bukan hanya perencanaan teknis, tetapi juga implementasi prinsip reliability dalam IoT security system.

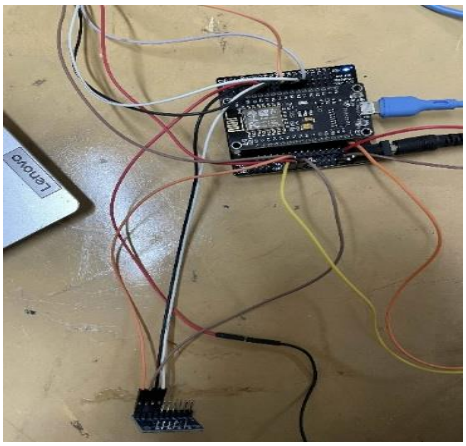
Rancangan komunikasi data yang ditetapkan pada tahap plan, yaitu sensor mengirim data ke NodeMCU lalu sistem menentukan respons berupa alarm, penguncian, dan notifikasi Telegram, merepresentasikan model closed-loop security control yang menjadi karakter utama sistem keamanan modern. Model ini selaras dengan temuan Oyon et al. (2025) yang menekankan bahwa integrasi Telegram Bot memungkinkan remote automation tidak hanya sebagai output pasif, tetapi sebagai kanal interaktif untuk kontrol perangkat secara langsung. Dalam penelitian ini, Telegram tidak diposisikan sekadar sebagai messenger, tetapi sebagai bagian dari ekosistem respons keamanan yang mempercepat intervensi pengguna. Studi Rambabu et al. (2025) juga menunjukkan bahwa motion-based security dengan Telegram notifications mampu meningkatkan kesiapsiagaan pengguna dalam menghadapi intrusi. Artinya, tahap plan telah menginternalisasi prinsip bahwa keamanan IoT harus berbasis respons cepat dan komunikasi dua arah.

Penggunaan sensor ultrasonik sebagai detektor pergerakan di sekitar brankas menegaskan bahwa penelitian ini mengadopsi pendekatan proximity-based threat detection, yang umum digunakan dalam smart surveillance berbasis ESP32-CAM maupun PIR motion sensor (Bagaskara & Susanto, 2025). Namun, berbeda dari pengawasan rumah terbuka, deteksi pergerakan pada brankas harus ditafsirkan lebih sensitif karena aktivitas kecil di sekitar brankas dapat menjadi indikator awal percobaan akses ilegal. Konsep early warning ini juga muncul dalam sistem monitoring keselamatan rumah tangga seperti deteksi kebocoran gas berbasis Telegram Bot, yang menekankan urgensi notifikasi instan ketika parameter abnormal terdeteksi (Afiyat et al., 2026). Dengan demikian, pemilihan HC-SR04 bukan sekadar komponen teknis, melainkan bagian dari strategi konseptual deteksi ancaman mikro dalam ruang domestik. Penempatan sensor ini dapat dilihat pada Gambar 2 Pemasangan Sensor Ultrasonik HC-SR04 sebagai bukti integrasi sistem input dalam prototipe.



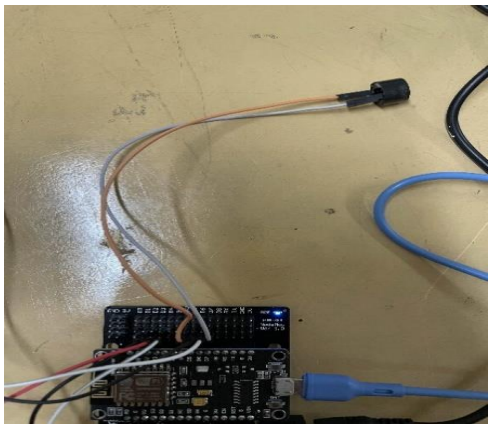
Gambar 2. Pemasangan Sensor Ultrasonik HC-SR04

Sementara itu, penggunaan MPU-6500 sebagai sensor getar memperkuat dimensi keamanan fisik yang sering diabaikan dalam studi IoT security berbasis notifikasi Telegram. Banyak penelitian sebelumnya lebih fokus pada deteksi visual atau motion detection eksternal melalui kamera ESP32-CAM (Jibin et al., 2025; Wicaksono et al., 2025), sedangkan ancaman terhadap brankas sering kali berbentuk hentakan atau pembongkaran paksa yang tidak selalu terdeteksi oleh sensor jarak. Dengan memasukkan sensor akselerasi multi-sumbu, penelitian ini memperluas paradigma intrusion detection menjadi physical tampering detection, yang lebih relevan untuk objek bernilai tinggi. Pendekatan ini sejalan dengan konsep sistem keamanan real-time berbasis sensor inersia yang digunakan dalam aplikasi keselamatan lain seperti fall detection untuk lansia (Riahi et al., 2025). Penempatan sensor MPU-6500 ditunjukkan pada Gambar 3 Foto Pemasangan Sensor MPU-6500, memperlihatkan bahwa sistem tidak hanya teoritis tetapi benar-benar terpasang pada struktur brankas.



Gambar 3. Foto pemasangan Sensor MPU-6500

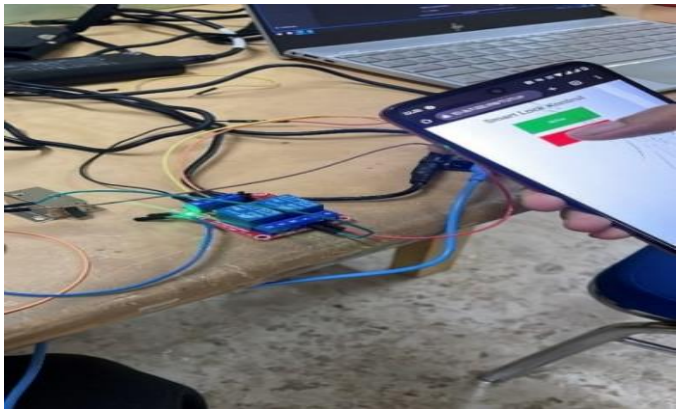
Dalam tahap plan, komponen buzzer sebagai alarm lokal juga memiliki signifikansi teoritis karena menghadirkan dual-layer security response: peringatan digital jarak jauh dan peringatan fisik langsung di lokasi. Literatur smart security menekankan bahwa sistem berbasis notifikasi mobile tetap memerlukan alarm lokal untuk meningkatkan deterrence effect terhadap pelaku intrusi (Fadhlurrohman & Basri, 2025). Dengan kata lain, buzzer tidak hanya berfungsi sebagai indikator suara, tetapi sebagai instrumen psikologis dalam strategi keamanan preventif. Hal ini konsisten dengan konsep multi-modal alerting dalam advanced monitoring solutions yang menggabungkan asisten digital dan Telegram Bot untuk memperkuat sistem peringatan (Sanjana et al., 2025). Penempatan buzzer dalam prototipe dapat dilihat pada Gambar 4. Foto Pemasangan Buzzer, yang memperlihatkan integrasi alarm dalam desain sistem.



Gambar 4. Foto pemasangan *Buzzer*

Solenoid door lock dan relay dalam tahap plan menunjukkan bahwa penelitian ini tidak berhenti pada deteksi ancaman, tetapi juga mengembangkan mekanisme respons otomatis berupa penguncian

elektronik. Sistem keamanan modern menuntut adanya automated access control agar ancaman tidak hanya diinformasikan, tetapi juga langsung dimitigasi melalui tindakan sistem (Sharma et al., 2025). Studi Putra Z. A. A. et al. (2025) pada RFID-based doorstop system juga menekankan pentingnya integrasi aktuator elektronik dengan Telegram untuk kontrol akses yang lebih aman. Dalam konteks brankas, solenoid menjadi bentuk physical enforcement yang memperkuat lapisan keamanan setelah ancaman terdeteksi. Implementasi rangkaian relay dan solenoid ditunjukkan pada Gambar 5. Rangkaian Solenoid Door Lock dan Relay, yang menegaskan bahwa sistem ini berbasis prototipe nyata. Tahap plan di sini menghubungkan teori access control dengan implementasi IoT berbasis aktuator.



Gambar 5. Rangkaian *Solenoid door lock* dan *Relay*

Perencanaan sistem monitoring berbasis Telegram Bot juga harus dipahami dalam lanskap perkembangan smart city ecosystem, di mana keamanan rumah menjadi bagian integral dari keamanan perkotaan berbasis jaringan. Wahyudi et al. (2025) menegaskan bahwa home security IoT bukan lagi sistem individual, tetapi node dalam ekosistem kota cerdas yang membutuhkan interoperabilitas dan komunikasi real-time. Dalam penelitian ini, Telegram Bot dipilih karena memiliki API yang fleksibel, ringan, dan mendukung notifikasi instan yang terbukti efektif dalam berbagai aplikasi IoT, mulai dari kontrol lampu rumah hingga sistem otomatis jemuran berbasis sensor cuaca (Dahana & Kurniawan, 2025; Kustiawan et al., 2025). Integrasi ini juga sejalan dengan paradigma low-cost scalable monitoring yang banyak diusulkan dalam sistem attendance dan security monitoring berbasis IoT-RFID-Webserver (Mayasari, 2025). Dengan demikian, tahap plan memperlihatkan bahwa penelitian ini tidak berdiri sendiri, tetapi relevan dengan diskursus smart infrastructure yang lebih luas. Telegram Bot dalam konteks ini diposisikan sebagai platform komunikasi universal dalam sistem keamanan domestik.

Keseluruhan tahapan prepare dan plan menunjukkan bahwa sistem monitoring keamanan brankas berbasis IoT yang dikembangkan dalam penelitian ini dibangun di atas sintesis literatur keamanan rumah, otomatisasi perangkat, serta notifikasi instan berbasis Telegram, tetapi dengan fokus yang lebih spesifik pada objek bernilai tinggi. Untuk memperjelas kebutuhan fungsional yang dirumuskan pada tahap prepare, berikut tabel ringkas yang ditempatkan dalam konteks analisis sistem:

Tabel 1. Kebutuhan Fungsional Sistem Monitoring Keamanan Brankas Berbasis IoT dan Komponen Pendukung

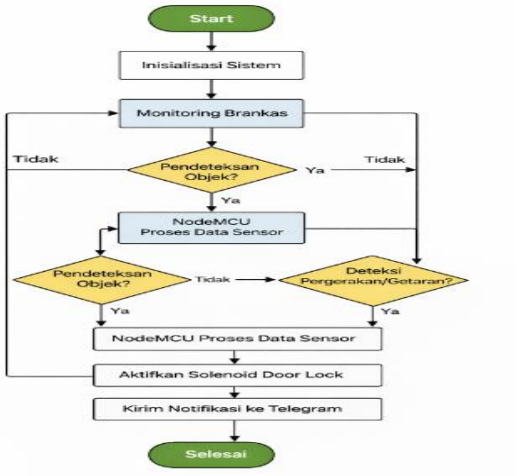
Kebutuhan Keamanan	Sensor/Aktuator Pendukung	Output Sistem
Deteksi Pergerakan	HC-SR04 Ultrasonik	Alarm + Notifikasi
Deteksi Getaran	MPU-6500	Alarm + Penguncian
Alarm Lokal	Buzzer	Peringatan Suara
Penguncian Otomatis	Solenoid + Relay	Brankas Terkunci
Notifikasi Real-Time	Telegram Bot + Website	Monitoring Jarak Jauh

Tabel ini menunjukkan bahwa pendekatan penelitian mengarah pada multi-layer security system yang menggabungkan sensing, alerting, dan physical locking dalam satu kesatuan, sebagaimana direkomendasikan dalam studi multisensor security prototype berbasis ESP32-CAM (Nannung & Miru,

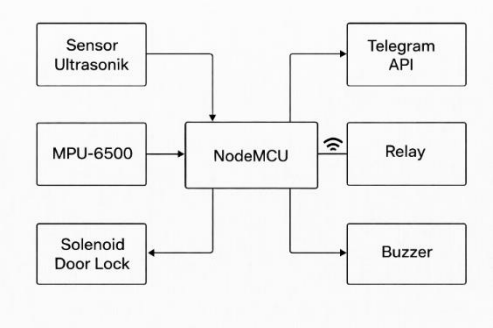
2025). Keunggulan utama rancangan ini terletak pada integrasi komponen deteksi ancaman mikro dengan sistem komunikasi instan, yang memperluas pendekatan IoT security beyond general home surveillance.

Tahap Design dan Implementasi Sistem sebagai Realisasi Arsitektur Keamanan Brankas Berbasis IoT

Tahap design dalam pengembangan sistem monitoring keamanan brankas berbasis IoT merupakan proses konseptualisasi teknis yang menjembatani kebutuhan fungsional pada tahap prepare–plan dengan realisasi sistem yang dapat bekerja secara operasional dalam konteks keamanan domestik. Pada tahap ini, rancangan arsitektur tidak hanya dipahami sebagai susunan komponen elektronik, tetapi sebagai representasi kerangka keamanan adaptif yang mengintegrasikan sensing, decision-making, dan alerting dalam satu siklus respons real-time. Literatur smart home security menekankan bahwa desain sistem yang efektif harus mampu meminimalkan jeda antara deteksi ancaman dan respons pengguna melalui notifikasi instan berbasis platform komunikasi yang ringan seperti Telegram (Suthar & Patel, 2025). Flowchart dan diagram blok yang disusun pada penelitian ini memperlihatkan bahwa sistem bekerja dalam model closed-loop monitoring, di mana input sensor diproses oleh mikrokontroler untuk menghasilkan output berupa alarm lokal, penguncian otomatis, dan notifikasi digital. Visualisasi desain tersebut ditunjukkan pada Gambar 6. Flowchart dan Gambar 7. Diagram Blok, yang menegaskan struktur sistem sebagai satu kesatuan arsitektur keamanan berbasis IoT.



Gambar 6. Flowchart



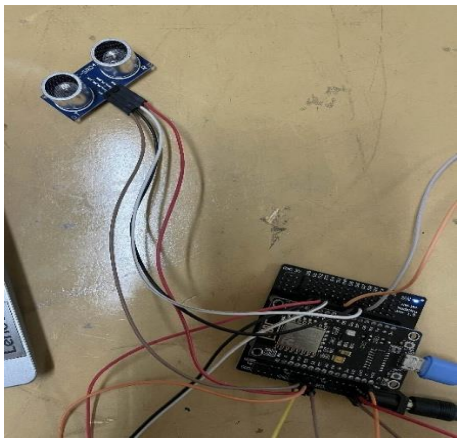
Gambar 7. Diagram Blok

Diagram blok sistem dalam penelitian ini menempatkan NodeMCU ESP8266 sebagai pusat pemrosesan yang berfungsi sebagai hub komunikasi antara sensor, aktuator, dan platform notifikasi, sehingga desain ini selaras dengan prinsip IoT edge computing yang mengutamakan pemrosesan cepat di tingkat perangkat sebelum data dikirim ke pengguna. Pendekatan ini relevan dengan temuan Kok et al. (2025) yang menekankan bahwa efisiensi energi dan sumber daya dalam sistem hazard detection IoT sangat bergantung pada kemampuan perangkat melakukan pemrosesan adaptif secara lokal. Dalam

konteks keamanan brankas, pemrosesan lokal menjadi krusial karena ancaman fisik memerlukan respons instan tanpa ketergantungan penuh pada cloud. Desain ini juga mengadopsi prinsip interoperabilitas smart city security ecosystem yang menghubungkan perangkat rumah tangga dengan komunikasi real-time (Wahyudi et al., 2025). Dengan demikian, tahap design memperlihatkan bahwa penelitian ini tidak sekadar merakit perangkat, tetapi membangun arsitektur keamanan berbasis teori IoT monitoring modern.

Flowchart sistem menggambarkan logika keputusan yang memastikan bahwa setiap perubahan parameter sensor langsung memicu aksi keamanan yang terprogram, sehingga sistem dapat berfungsi sebagai early warning mechanism terhadap aktivitas mencurigakan. Hal ini konsisten dengan pendekatan intrusion detection berbasis mobile notifications yang menekankan pentingnya jalur keputusan otomatis dalam sistem keamanan (Medina-Ángel & Burlak, 2025). Pada sistem ini, ketika sensor ultrasonik mendeteksi perubahan jarak signifikan atau sensor MPU-6500 membaca akselerasi abnormal, NodeMCU segera mengaktifkan buzzer dan mengunci solenoid door lock sebelum notifikasi dikirim melalui Telegram. Pendekatan semacam ini menunjukkan bahwa desain penelitian tidak hanya informatif tetapi juga preventif, karena sistem melakukan mitigasi fisik secara otomatis. Konsep ini sejalan dengan studi Sharma et al. (2025) tentang portable door lock system berbasis Telegram Bot yang menekankan penguatan akses kontrol melalui automasi.

Implementasi sensor ultrasonik HC-SR04 dalam sistem ini memperlihatkan bahwa deteksi ancaman berbasis proximity menjadi komponen penting dalam monitoring keamanan brankas, karena pergerakan kecil di sekitar objek bernilai tinggi dapat menjadi indikator awal percobolan. Studi Bagaskara dan Susanto (2025) menunjukkan bahwa motion sensor dan kamera ESP32-CAM efektif untuk pengawasan rumah, namun dalam konteks brankas, sensor jarak memberikan pendekatan lebih sederhana tetapi responsif untuk mendeteksi interaksi langsung. Sensor HC-SR04 dipasang pada area internal brankas untuk memantau perubahan jarak objek yang mendekat, sebagaimana ditunjukkan pada Gambar 8. Pemasangan Sensor Ultrasonik HC-SR04. Integrasi ini memperlihatkan bahwa desain sistem mengarah pada micro-surveillance yang fokus pada ruang terbatas, bukan monitoring area luas. Dengan demikian, implementasi sensor ini menjadi adaptasi penting dari konsep smart surveillance ke keamanan objek spesifik.



Gambar 8. Pemasangan Sensor Ultrasonik HC-SR04

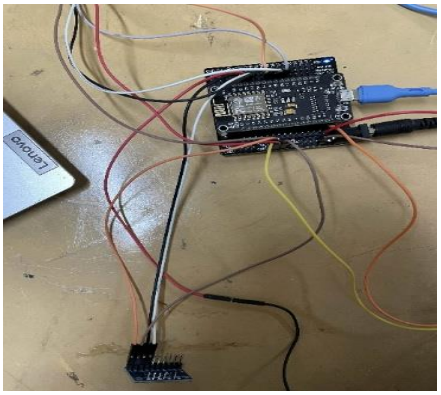
Pengujian sensor HC-SR04 menghasilkan rata-rata error ±1,6 cm, yang menunjukkan bahwa sensor cukup akurat dalam rentang threshold ≤30 cm untuk mendeteksi aktivitas mencurigakan, namun memiliki keterbatasan pada jarak lebih jauh yang dapat memicu false negative. Temuan ini menguatkan argumen bahwa sistem IoT security harus mengandalkan parameter ambang yang dikalibrasi secara kontekstual agar respons sistem tetap valid dan tidak over-sensitive (Kok et al., 2025). Untuk memperjelas performa sensor, data uji berikut ditempatkan dalam konteks evaluasi:

Tabel 2. Ringkasan Hasil Pengujian Sensor Ultrasonik HC-SR04 terhadap Deteksi Pergerakan

Jarak Aktual (cm)	Jarak Terbaca (cm)	Error (cm)	Status
10	11	1	Deteksi
20	21	1	Deteksi
30	32	2	Tidak

Data ini menunjukkan bahwa pada jarak mendekati batas threshold, error meningkat dan status deteksi menjadi tidak konsisten, sehingga kalibrasi sensor menjadi bagian penting dari optimasi desain. Studi Salsabila et al. (2025) juga menekankan bahwa sistem keamanan pintu berbasis smart detection memerlukan penyesuaian threshold agar tidak menimbulkan alarm palsu. Dengan demikian, hasil ini tidak hanya bersifat teknis tetapi juga memiliki implikasi metodologis dalam desain sistem keamanan berbasis sensor jarak.

Implementasi sensor MPU-6500 memberikan dimensi keamanan tambahan yang berfokus pada deteksi guncangan atau hentakan fisik sebagai indikator percobaan pembobolan brankas. Berbeda dengan penelitian surveillance berbasis kamera yang dominan dalam literatur (Jibin et al., 2025; Rambabu et al., 2025), pendekatan inersia ini lebih relevan untuk objek tertutup yang tidak selalu memerlukan pemantauan visual. Sensor dipasang pada sisi badan brankas sebagaimana ditunjukkan pada Gambar 9. Foto Pemasangan Sensor MPU-6500, sehingga dapat menangkap percepatan multi-sumbu secara real-time. Respons sensor yang cepat, yaitu 0,2–0,5 detik, memperlihatkan potensi sistem dalam memberikan peringatan dini sebelum terjadi kerusakan fisik lebih lanjut. Pendekatan ini juga paralel dengan penggunaan sensor percepatan dalam sistem keselamatan real-time seperti fall detection yang memerlukan respons cepat berbasis akselerasi (Riahi et al., 2025).



Gambar 9. Foto pemasangan Sensor MPU-6500

Data pengujian MPU-6500 menunjukkan bahwa sensor mampu membedakan antara sentuhan ringan yang tidak berbahaya dan hentakan kuat yang mengindikasikan ancaman, sehingga sistem dapat mengurangi alarm palsu dan meningkatkan reliabilitas monitoring. Hal ini relevan dengan prinsip adaptive monitoring yang menuntut sistem mampu mengklasifikasikan tingkat ancaman berdasarkan intensitas sinyal sensor (Kok et al., 2025). Data berikut memperlihatkan pola tersebut secara empiris:

Tabel 3. Hasil Pengujian Sensor Getar MPU-6500 Berdasarkan Intensitas Akselerasi

Jenis Getaran	Nilai Akselerasi (g)	Status
Sentuhan ringan	0.15	Tidak
Ketukan sedang	0.42	Deteksi
Hentakan kuat	0.88	Deteksi

Hasil ini menunjukkan bahwa ancaman fisik dapat diidentifikasi secara kuantitatif melalui ambang akselerasi tertentu, yang memperkuat argumen bahwa keamanan brankas membutuhkan sensor tampering khusus, bukan hanya motion detection eksternal. Studi Nannung dan Miru (2025) juga

menekankan pentingnya pendekatan multisensor untuk meningkatkan akurasi deteksi ancaman. Dengan demikian, MPU-6500 berperan sebagai komponen konseptual dalam memperluas definisi intrusion detection pada sistem brankas.

Implementasi buzzer sebagai alarm lokal dan solenoid door lock sebagai mekanisme penguncian otomatis menunjukkan bahwa sistem ini mengadopsi strategi layered defense, yaitu kombinasi deterrence lokal dan mitigasi akses fisik. Studi Fadhlurrohman dan Basri (2025) menegaskan bahwa sistem anti theft berbasis Telegram harus tetap memiliki alarm suara untuk memberikan efek preventif langsung terhadap pelaku. Solenoid door lock yang dikendalikan relay juga memperlihatkan bahwa sistem mampu melakukan physical enforcement secara otomatis, sebagaimana konsep access control dalam sistem pintu pintar berbasis Telegram Bot (Putra Z. A. A. et al., 2025). Implementasi rangkaian ini ditunjukkan pada Gambar 5. Rangkaian Solenoid Door Lock dan Relay, yang memperkuat validitas prototipe. Dengan demikian, sistem tidak hanya mendeteksi ancaman tetapi juga melakukan tindakan keamanan aktif.

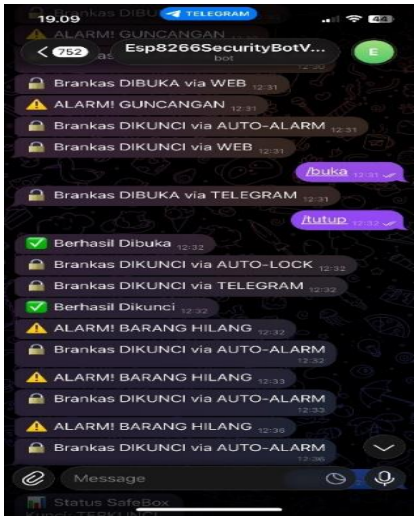
Pengujian solenoid door lock menunjukkan tingkat keberhasilan 100% dalam seluruh skenario uji, yang mengindikasikan bahwa aktuator ini cukup stabil untuk mendukung mekanisme penguncian otomatis berbasis deteksi sensor. Data berikut menegaskan performa tersebut dalam konteks waktu aktif:

Tabel 4. Performa Solenoid Door Lock dalam Berbagai Skenario Penguncian Otomatis

Skenario Uji	Waktu Aktif (detik)	Status
Deteksi getaran	0.28	Berhasil
Deteksi pergerakan	0.30	Berhasil
Perintah manual (web)	0.35	Berhasil

Keberhasilan ini memperlihatkan bahwa sistem mampu merespons ancaman fisik maupun perintah digital dengan latensi rendah, yang menjadi indikator penting dalam IoT security system berbasis real-time (Antono & Suryo, 2025). Studi Putra F. P. et al. (2025) juga menegaskan bahwa kontrol perangkat IoT melalui Telegram Bot memerlukan aktuator yang stabil agar perintah jarak jauh dapat dieksekusi secara konsisten. Dengan demikian, hasil ini memperkuat kontribusi metodologis penelitian dalam membangun sistem keamanan brankas yang dapat diandalkan.

Integrasi Telegram Bot sebagai media notifikasi real-time memperlihatkan bahwa desain dan implementasi sistem ini sejalan dengan tren global penggunaan instant messaging sebagai platform utama dalam smart security monitoring. Studi Suthar dan Patel (2025) serta Afiyat et al. (2026) menegaskan bahwa Telegram Bot menawarkan latensi rendah dan fleksibilitas tinggi untuk berbagai aplikasi monitoring rumah tangga. Notifikasi sistem ditampilkan pada Gambar 10. Tampilan Notifikasi Telegram, sementara waktu pengiriman pesan rata-rata 1,33 detik menunjukkan bahwa sistem mampu memberikan respons digital yang cukup cepat untuk konteks keamanan domestik. Data berikut memperlihatkan variasi latensi notifikasi:



Gambar 10. Tampilan notifikasi Telegram

Tabel 5. Waktu Latensi Pengiriman Notifikasi Sistem melalui Telegram Bot

Skenario Notifikasi	Waktu Kirim (detik)
Getaran terdeteksi	1.2
Solenoid terkunci via Telegram	1.0
Solenoid terkunci via Website	1.3

Temuan ini menegaskan bahwa kualitas koneksi internet tetap menjadi faktor eksternal yang mempengaruhi performa sistem IoT real-time, sebagaimana juga dicatat dalam berbagai studi monitoring berbasis Telegram untuk otomasi perangkat rumah (Dahana & Kurniawan, 2025; Kustiawan et al., 2025). Dengan demikian, tahap design dan implementasi dalam penelitian ini menunjukkan integrasi konseptual dan teknis yang kuat antara sensor-based intrusion detection, automated locking, serta komunikasi instan melalui Telegram Bot sebagai bentuk modern smart security architecture.

Tahap Operate dan Optimize sebagai Evaluasi dan Penyempurnaan Sistem Monitoring Keamanan Brankas Berbasis IoT

Tahap *operate* dalam pengembangan sistem monitoring keamanan brankas berbasis Internet of Things (IoT) merupakan fase implementasi nyata yang menempatkan prototipe pada konteks penggunaan sesungguhnya untuk menguji kestabilan fungsi deteksi ancaman dan efektivitas respons sistem secara real-time. Pada tahap ini, sistem tidak lagi dipahami sebagai rancangan konseptual, melainkan sebagai perangkat keamanan domestik yang harus mampu bekerja konsisten dalam kondisi lingkungan dinamis, variasi ancaman fisik, serta fluktuasi jaringan komunikasi. Pengujian operasional dilakukan melalui skenario ancaman seperti percobaan pembukaan paksa, guncangan pada brankas, dan pergerakan mencurigakan di sekitar objek, sehingga memungkinkan evaluasi menyeluruh terhadap integrasi sensor ultrasonik, sensor MPU-6500, buzzer, dan solenoid door lock. Literatur keamanan IoT menekankan bahwa tahap operate menjadi titik kritis karena validitas sistem hanya dapat dibuktikan melalui pengamatan langsung terhadap kinerja end-to-end, bukan hanya melalui simulasi laboratorium (Wahyudi et al., 2025). Implementasi ini memperlihatkan bahwa sistem mampu menjalankan fungsi utama berupa deteksi ancaman dan aktivasi pengamanan secara simultan dalam kondisi nyata.

Evaluasi tahap operate juga menekankan pentingnya sinkronisasi komunikasi data antara perangkat NodeMCU ESP8266 dan platform notifikasi Telegram Bot, karena sistem keamanan berbasis IoT menuntut penyampaian informasi ancaman tanpa jeda signifikan agar pengguna dapat mengambil keputusan cepat. Penelitian terdahulu menunjukkan bahwa Telegram Bot semakin banyak digunakan sebagai media komunikasi keamanan rumah karena bersifat instan, ringan, dan dapat diakses lintas perangkat (Suthar & Patel, 2025). Dalam penelitian ini, sistem diuji untuk memastikan bahwa notifikasi dapat dikirim segera setelah sensor mendeteksi perubahan jarak atau getaran abnormal, sekaligus mengaktifkan buzzer sebagai alarm lokal. Temuan ini sejalan dengan studi Fadhlurrohman dan Basri

(2025) yang menegaskan bahwa integrasi notifikasi berbasis bot memperkuat sistem anti-theft karena memberikan peringatan jarak jauh yang responsif. Dengan demikian, tahap operate memperlihatkan bahwa sistem monitoring brankas tidak hanya bekerja secara lokal, tetapi juga mampu membangun komunikasi keamanan real-time berbasis jaringan.

Tahap *optimize* dilakukan setelah evaluasi operasional menunjukkan bahwa sistem keamanan IoT memerlukan penyempurnaan parameter teknis agar lebih stabil dan akurat dalam menghadapi kondisi lingkungan yang bervariasi. Optimasi difokuskan pada pengaturan ambang batas sensor getar MPU-6500 untuk mengurangi noise serta meminimalkan alarm palsu yang dapat terjadi akibat getaran ringan non-ancaman. Literatur intrusion detection berbasis sensor menekankan bahwa sistem keamanan yang terlalu sensitif justru menurunkan kepercayaan pengguna karena memicu false alarm secara berulang (Rambabu et al., 2025). Selain itu, optimasi juga dilakukan pada mekanisme komunikasi Telegram dengan menambahkan logika pengiriman ulang pesan apabila terjadi gangguan jaringan, sehingga sistem tidak gagal menyampaikan peringatan saat ancaman nyata muncul (Afiyat et al., 2026). Dengan demikian, optimize menjadi fase strategis yang memperkuat reliabilitas sistem melalui penyempurnaan perangkat lunak dan penyesuaian konfigurasi sensor.

Tahap operate dan optimize membuktikan bahwa sistem monitoring keamanan brankas berbasis IoT yang dikembangkan telah mampu bekerja secara real-time melalui integrasi sensor, aktuator pengunci otomatis, alarm suara, serta notifikasi Telegram Bot sebagai media komunikasi utama. Tahap operate menunjukkan bahwa sistem berhasil mendeteksi ancaman fisik dan memberikan respons cepat, sedangkan tahap optimize memastikan bahwa performa sistem semakin stabil dengan mengurangi alarm palsu dan meningkatkan keandalan komunikasi data. Studi-studi terbaru dalam bidang smart home security menegaskan bahwa efektivitas sistem keamanan modern bergantung pada kemampuan adaptasi parameter dan evaluasi berkelanjutan, bukan sekadar keberhasilan rancang bangun awal (Jibin et al., 2025). Dengan demikian, penelitian ini tidak hanya menghasilkan prototipe pengamanan brankas, tetapi juga menawarkan model pengembangan sistem keamanan domestik berbasis IoT yang terukur, responsif, dan siap diimplementasikan pada skala rumah tangga.

KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem monitoring keamanan brankas rumah berbasis Internet of Things (IoT) secara real-time melalui integrasi NodeMCU ESP8266, sensor ultrasonik HC-SR04, sensor getar MPU-6500, buzzer, solenoid door lock, serta notifikasi Telegram Bot dan web monitoring. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi pergerakan dengan rata-rata error ±1,6 cm dan mendeteksi getaran signifikan dengan waktu respons 0,2–0,5 detik, sementara mekanisme penguncian otomatis solenoid menunjukkan tingkat keberhasilan 100% dalam seluruh skenario uji. Notifikasi Telegram dapat dikirim dengan latensi rata-rata 1,33 detik, menegaskan kemampuan sistem dalam memberikan peringatan dini kepada pengguna secara cepat dan jarak jauh. Tahap optimasi melalui kalibrasi sensor, penyesuaian threshold, serta stabilisasi koneksi jaringan memperkuat reliabilitas sistem dan mengurangi potensi alarm palsu. Dengan demikian, sistem yang dikembangkan memberikan kontribusi praktis sebagai solusi keamanan domestik yang adaptif, responsif, dan relevan untuk mendukung penguatan ekosistem smart home security berbasis IoT.

DAFTAR PUSTAKA

Afiyat, N., Pramartaningthyas, E. K., & Prasetyo, A. (2026). IoT-Based LPG Gas Leak Detection System for Real-Time Household Safety Monitoring Integrated with Telegram Bot Notifications. *G-Tech: Jurnal Teknologi Terapan*, *10*(1), 140-151. https://doi.org/10.70609/g-tech.v10i1.8650

Antono, D. R. R., & Suryo, Y. A. (2025). Security System in A Private Room Using Esp32 Microcontroller with Telegram Bot. *Journal of Energy and Electrical Engineering*, *6*(2). https://doi.org/10.37058/jeee.v6i2.14951

Bagaskara, A. R., & Susanto, A. (2025). Design of an Internet of Things (IoT) Based Security System Using Esp32 Cam and Passive Infrared Receiver (PIR) Motion Sensor in the Home Environment. *International Journal of Engineering Computing Advanced Research*, *2*(1), 11-18. https://journals.arces.org/ijecar/article/view/90

Dahana, G., & Kurniawan, H. (2025, December). Rancang Bangun Sistem Pengendalian Lampu Rumah Berbasis Iot Terintegrasi Dengan Telegram. In *PROSIDING SEMINAR NASIONAL MULTI DISIPLIN ILMU (SENADIMU)* (Vol. 2, No. 1, pp. 24-37).

Fadhlurrohman, D., & Basri, M. (2025). Home Anti Theft System Uses Based Telegram Bot Internet of Things. *Hanif Journal of Information Systems*, *3*(1), 1-8. https://doi.org/10.56211/hanif.v3i1.36

Faturohman, A. C. (2025, December). Detection and Telegram Messages using ESP32-Wrover. In *Proceedings of the 8th International Conference on Informatics, Engineering, Science & Technology (INCITEST 2025)* (p. 37). Springer Nature.

Jibin, G., Shihabudeen, H., Vignesh, S., Akhil, A., Deepak, V. K., & Juliemol, P. M. (2025, July). SmartGuard: An IoT-based Home Surveillance System using ESP32-CAM and Telegram. In *2025 8th International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 458-463). IEEE. https://ieeexplore.ieee.org/abstract/document/11140951

Kok, C. L., Heng, J. B., Koh, Y. Y., & Teo, T. H. (2025). Energy-, Cost-, and Resource-Efficient IoT Hazard Detection System with Adaptive Monitoring. *Sensors*, *25*(6), 1761. https://doi.org/10.3390/s25061761

Kustiawan, H. B., Sudibyo, H., & Winarti, D. (2025). Development of an Automatic Clothesline System Based on Weather Sensors and Telegram Notification. *bit-Tech*, *8*(2), 1357-1366. https://doi.org/10.32877/bt.v8i2.2900

Mayasari, A. (2025). Real-Time Attendance and Security Monitoring System Using IoT-RFID-Webserver-Android: A Low-Cost Solution. *International Journal on Advanced Science, Engineering & Information Technology*, *15*(3).

Medina-Ángel, G., & Burlak[1], G. (2025, March). Intrusion Detection System Through Mobile Notifications Using the Internet. In *Smart Cities: 7th Ibero-American Congress, ICSC-CITIES 2024, San Carlos, Costa Rica, November 12–14, 2024, Revised Selected Papers* (Vol. 2394, p. 89). Springer Nature.

Nannung, J., & Miru, A. S. B. (2025). Development of an IoT-Based Home Security System Prototype Using Multisensors and ESP32-CAM. *Journal of Embedded Systems, Security and Intelligent Systems*, 168-177. https://journal.unm.ac.id/index.php/JESSI/article/view/8456

Oyon, M. S. S., Himel, A. H., Mredul, K., Ahmed, A., Ali, M. T., Hossainl, C. A., & Rahman, M. A. (2025, January). Design and Optimization of an IR-Based Automation System with Telegram Bot Integration for Remote Device Control. In *2025 4th International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)* (pp. 275-279). IEEE. https://ieeexplore.ieee.org/abstract/document/10914456

Putra, F. P., Sabirin, S., & Soetanto, H. (2025). Prototype of Internet of Things-Based Control System Using Telegram with Bot API Method. *Jurnal Syntax Transformation*, *6*(2), 87-109. https://doi.org/10.46799/jst.v6i2.1055

Putra, Z. A. A., Adek, R. T., & Aidilof, H. A. K. (2025). Design and Implementation of an RFID-Based Automatic Doorstop System with Website and Telegram Bot Integration. *Tech-E*, *8*(2), 125-140. https://doi.org/10.31253/te.v8i2.3447

Rambabu, K., Karthik, K., Sai, G. R., & Kumar, K. H. (2025, September). Design and Deploy an ESP32-CAM Motion Security System with Telegram Notifications. In *2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 213-220). IEEE. https://ieeexplore.ieee.org/abstract/document/11212532

Riahi, T., Bappy, M. A. H., & Islam, M. M. (2025). ElderFallGuard: Real-Time IoT and Computer Vision-Based Fall Detection System for Elderly Safety. *arXiv preprint arXiv:2505.11845*. https://doi.org/10.48550/arXiv.2505.11845

Salsabila, N., Siswanto, A., & Bayuaji, L. (2025, January). Design of a smart home door security system with face detection and smart bell using esp32-cam. In *2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)* (pp. 124-129). IEEE. https://ieeexplore.ieee.org/abstract/document/10883160

Sanjana, B., Sathya, L., Narayanan, G. S., Rasool, A. A., & Padmavathi, B. (2025, August). Advanced Monitoring Solutions with Google Assistant and Telegram Bot: A Focus on Solidified Carbon Dioxide (CO 2). In *2025 3rd International Conference on Sustainable Computing and Data*

Communication Systems (ICSCDS) (pp. 1331-1338). IEEE. https://ieeexplore.ieee.org/abstract/document/11167657

Sharma, V., Suneja, P., & Shokeen, S. (2025). Portable Door Lock System using Telegram Bot. *Available at SSRN 5909222*.

Suthar, D., & Patel, M. (2025, April). IoT-Based Home Security System Using Telegram. In *2025 12th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 1-9). IEEE. https://ieeexplore.ieee.org/abstract/document/11115737

Vamshi, V., Pankaj, C., Dhanush, R., & Manohara, H. T. (2025, September). Design and Development of Real-time Four-legged Robot for Security Applications. In *2025 IEEE North Karnataka Subsection Flagship International Conference (NKCon)* (pp. 1-6). IEEE. https://ieeexplore.ieee.org/abstract/document/11345773

Wahyudi, A. D., Astawa, I. G. P., & Nadziroh, F. (2025). Development of IoT-Based Home Security Monitoring and Management Systems to Support Smart City Ecosystems. *The Indonesian Journal of Computer Science*, *14*(2). https://doi.org/10.33022/ijcs.v14i2.4605

Wicaksono, M. F., Rahmatya, M. D., & Faturohman, A. C. (2025, December). Smart Home Monitoring and Control with Human Detection and Telegram Messages using ESP32-Wrover CAM. In *8th International Conference on Informatics, Engineering, Science & Technology (INCITEST 2025)* (pp. 37-53). Atlantis Press. https://doi.org/10.2991/978-94-6463-924-7_5