

Kotak Amal Pintar Berbasis *Internet of Things* (IoT) Menggunakan *Platform Blynk* di SMAN 1 Serangpanjang

Asep Soendara¹, Kodar Udoyono¹, Eka Permana^{1*}, Setia Aji¹, Daud Elia
Leander¹, Akrom Muhajir²

¹Teknik Komputer dan Jaringan, Fakultas Teknik, Universitas Mandiri, Indonesia

²Teknik Informatika, Fakultas Teknik, Universitas Mandiri, Indonesia

E-mail: asepsoundara@gmail.com¹, kodarudoyono85@gmail.com¹, exadoak@gmail.com¹,
setia.aji.bdg@gmail.com¹, daudelialeander@gmail.com¹, akrommuhajir1986@gmail.com²

Received: 2025-09-11 | Accepted: 2025-09-20 | Published: 2025-10-01

Abstrak

Penelitian ini bertujuan untuk mengembangkan kotak amal berbasis *Internet of Things* (IoT) yang dapat dimonitoring dan dikendalikan secara daring melalui *platform Blynk*. Kotak amal konvensional umumnya masih mengandalkan metode perhitungan manual yang rentan terhadap manipulasi dan kesalahan, serta kelemahan penggunaan kunci tradisional, seperti risiko kehilangan atau duplikasi yang tidak sah. Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan sebuah sistem berbasis IoT yang dirancang guna meningkatkan transparansi dan keamanan.

Metode penelitian yang digunakan meliputi studi literatur untuk memahami konsep IoT dan teknologi yang relevan, serta peninjauan terhadap perangkat *RFID reader* dan sensor warna. Selain itu, dilakukan analisis kebutuhan pengguna dan perancangan sistem untuk memastikan ketersediaan informasi yang akurat dan sesuai kebutuhan. Hasil yang diharapkan dari penelitian ini adalah terciptanya prototipe yang mampu memantau kondisi keamanan kotak amal secara *realtime*, sehingga keandalan serta keamanan donasi dapat lebih terjamin. Penelitian ini juga diharapkan dapat menjadi referensi bagi penelitian selanjutnya yang berfokus pada pengembangan sistem keamanan berbasis IoT.

Kata Kunci: *Blynk, Internet of Things, RFID Reader, Sensor Getar.*

Abstract

The objective of this study is to develop an Internet of Things (IoT)-based donation box that can be monitored and controlled remotely through the Blynk platform. Conventional donation boxes typically rely on manual counting methods, which are prone to manipulation and errors, as well as vulnerabilities related to the use of traditional keys, such as loss or unauthorized duplication. To address these issues, this research proposes an IoT-enabled system designed to enhance both transparency and security. The research methodology includes a literature survey to understand IoT concepts and relevant technologies, as well as an evaluation of RFID readers and color sensors. Additionally, user requirements analysis and system design were conducted to ensure the accurate and relevant delivery of information. The expected outcome of this study is a prototype that enables real-time monitoring of donation box security, thereby improving reliability and safeguarding donations. Furthermore, this work is expected to serve as a reference for future research related to IoT-based security systems.

Keywords: *Blynk, Internet of Things, RFID Reader, Vibration Sensor.*

1. Pendahuluan

Pengelolaan kotak amal secara manual masih menghadapi berbagai kendala, antara lain perhitungan donasi yang dilakukan secara manual yang rawan kesalahan atau manipulasi serta penggunaan kunci mekanik yang dapat hilang atau dipalsukan. Dengan kemajuan teknologi *Internet of Things* (IoT), terdapat potensi besar untuk meningkatkan keamanan dan transparansi dalam sistem kotak amal [1].

Teknologi sensor dan komunikasi jarak jauh melalui platform IoT memungkinkan pemantauan secara *realtime* terhadap kondisi fisik kotak amal, seperti adanya getaran atau gangguan fisik, serta identifikasi akses menggunakan RFID. Misalnya, penggunaan sensor getar (*vibration sensor*) sebagai pendeteksi pergerakan abnormal dapat memicu alarm atau notifikasi ke pengelola [2], sedangkan penggunaan RFID reader memungkinkan identifikasi pihak yang mengakses kotak tanpa memerlukan kunci mekanik [3].



Platform aplikasi seperti Blynk telah digunakan dalam berbagai proyek IoT sebagai media antarmuka pengguna untuk monitoring waktu nyata dan kontrol jarak jauh perangkat IoT, termasuk dalam proyek celengan pintar dan kotak donasi [4]. Integrasi sensor-sensor (misalnya sensor warna, sensor getar, RFID reader) bersama mikrokontroler dan konektivitas internet membuka kemungkinan untuk sistem yang tidak hanya aman tetapi juga ramah pengguna dan efisien [5].

Di Indonesia, beberapa penelitian telah dilakukan terkait sistem keamanan kotak amal berbasis IoT. Misalnya, integrasi sensor getar dan *pin lock* untuk keamanan kotak amal [6], penggunaan sensor warna dengan platform Firebase dan bot Telegram untuk transparansi donasi [7], serta rancangan sistem kamera keamanan berbasis IoT dan Telegram [8]. Lebih lanjut, penelitian internasional juga menyoroti penggunaan sensor PIR (HC-SR501) dan sensor magnetik (MC-38) dalam mendeteksi pencurian pada kotak amal [9].

Selain itu, aspek keamanan RFID menjadi perhatian penting dalam aplikasi IoT modern. Evaluasi keamanan dan *reverse engineering* terhadap tag RFID komersial menunjukkan bahwa teknologi ini perlu diimplementasikan dengan mekanisme proteksi tambahan agar tidak mudah disalahgunakan [10].

Berdasarkan tinjauan tersebut, masih terdapat kebutuhan untuk sistem kotak amal yang lebih komprehensif, dengan menggabungkan kontrol akses berbasis RFID, pemantauan kondisi fisik (misalnya getaran), kamera atau sensor tambahan, serta antarmuka pengguna berbasis aplikasi mobile seperti Blynk. Penelitian ini bertujuan merancang dan mengimplementasikan Kotak Amal Pintar berbasis IoT di SMAN 1 Serangpanjang, sehingga keamanan kotak amal dapat lebih terjaga, manipulasi dapat diminimalisir, dan pengelolaan donasi menjadi lebih transparan serta efisien.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan rekayasa perangkat keras dan perangkat lunak berbasis Internet of Things (IoT). Metode yang diterapkan terdiri atas beberapa tahapan, yaitu: studi literatur, analisis kebutuhan, perancangan sistem, implementasi, serta pengujian dan evaluasi.

1. Studi Literatur

Tahap awal dilakukan dengan mengkaji literatur terkait konsep IoT, keamanan sistem berbasis sensor, serta teknologi yang mendukung pengembangan kotak amal pintar. Beberapa penelitian sebelumnya menjadi acuan, seperti penerapan sensor getar dan RFID untuk keamanan kotak amal [2], [3], penggunaan platform Blynk sebagai antarmuka monitoring IoT [4], serta integrasi Firebase dan bot Telegram untuk transparansi donasi [7].

2. Analisis Kebutuhan

- Analisis kebutuhan dilakukan melalui observasi terhadap permasalahan kotak amal konvensional di SMAN 1 Serangpanjang. Masalah utama yang teridentifikasi adalah potensi manipulasi perhitungan manual, kelemahan kunci mekanik, serta tidak adanya sistem monitoring secara *realtime*. Dari hasil analisis, kebutuhan utama meliputi:
- Perangkat keras: mikrokontroler (NodeMCU ESP8266), sensor getar, RFID reader, dan kunci solenoid.
- Perangkat lunak: aplikasi Blynk untuk monitoring dan kontrol, serta protokol komunikasi berbasis Wi-Fi.
- Fungsionalitas: sistem harus mampu mendeteksi akses melalui RFID, memantau getaran atau percobaan pembobolan, serta menampilkan status kotak amal secara *realtime* di aplikasi.

3. Perancangan Sistem

- Perancangan sistem meliputi desain perangkat keras dan perangkat lunak:
- Perangkat keras: RFID reader digunakan sebagai kontrol akses utama; sensor getar untuk mendeteksi upaya pembobolan; NodeMCU sebagai pengendali utama yang menghubungkan sensor dengan server IoT.
- Perangkat lunak: aplikasi Blynk dikonfigurasi untuk menerima data dari NodeMCU, menampilkan status kotak amal, serta mengirim notifikasi jika terjadi aktivitas mencurigakan. Diagram blok sistem dapat digambarkan sebagai hubungan antara modul RFID, sensor getar, NodeMCU, server Blynk, dan perangkat pengguna (smartphone).

4. Implementasi

Tahap implementasi dilakukan dengan merakit perangkat keras sesuai rancangan dan memprogram mikrokontroler menggunakan Arduino IDE. NodeMCU diprogram untuk membaca data dari RFID reader dan sensor getar, kemudian mengirimkan informasi ke aplikasi Blynk melalui koneksi Wi-Fi. Aplikasi Blynk diatur agar dapat menampilkan status kotak amal, jumlah akses, serta memberikan notifikasi alarm saat terjadi getaran abnormal.

5. Pengujian dan Evaluasi

Pengujian dilakukan dengan metode *black box* pada setiap modul:

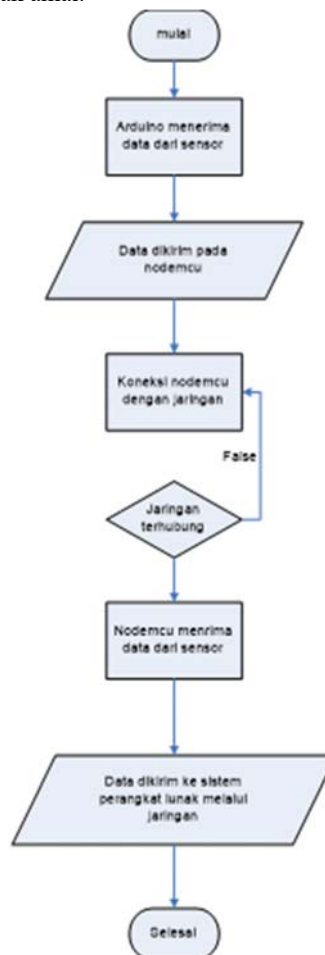
- Pengujian RFID untuk memastikan hanya kartu terdaftar yang dapat membuka kunci solenoid.
- Pengujian sensor getar untuk menguji sensitivitas terhadap benturan atau guncangan.
- Pengujian komunikasi NodeMCU–Blynk untuk memastikan data dikirim dan diterima secara *realtime*.
- Pengujian sistem keseluruhan untuk mengevaluasi keandalan, keamanan, dan kinerja prototipe kotak amal pintar.

Evaluasi hasil dilakukan dengan membandingkan fungsi sistem terhadap kebutuhan pengguna. Hasil pengujian diharapkan menunjukkan bahwa sistem mampu memberikan informasi keamanan kotak amal secara *realtime*, mengurangi risiko manipulasi, dan meningkatkan transparansi pengelolaan donasi.

3. Hasil dan Pembahasan

3.1. Alur Sistem

Prototipe kotak amal pintar berhasil dirancang menggunakan mikrokontroler NodeMCU ESP8266 sebagai pusat pengendali. Perangkat keras utama yang digunakan terdiri atas RFID reader, sensor getar, kunci solenoid, dan catu daya. Semua komponen dirakit pada kotak akrilik berukuran $30 \times 20 \times 20$ cm yang berfungsi sebagai wadah simulasi kotak amal.



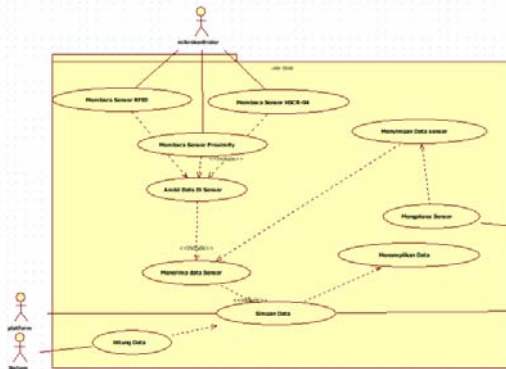
Gambar 1. Flowchart

Arduino menerima dari setiap sensor, proses pengiriman data ke sistem dengan menggunakan jaringan melalui NodeMCU. Jika proses pengiriman data tidak terhubung dengan jaringan, maka proses kembali ke awal. Tapi jika terhubung dengan jaringan maka proses pengiriman data ke sistem berhasil.

Dari sisi perangkat lunak, aplikasi Blynk berhasil dikonfigurasi untuk menampilkan status kotak amal secara *realtime*. Dashboard pada aplikasi terdiri dari indikator status kotak (terkunci/terbuka), log akses RFID, serta notifikasi alarm saat terjadi getaran.

3.2. Use Case

Actor yang memiliki tanggung jawab pada *use case* yaitu Mikrokontroler, Platform, Sistem, dan User, setiap actor memiliki tugas masing-masing sesuai dengan hak akses terhadap sistem. *Use case* diagram dapat dilihat pada gambar 2.



Gambar 2. Use Case Diagram

Diagram *Use Case* ini memodelkan interaksi fungsional inti dalam sebuah sistem otomatis yang berfokus pada Mikrokontroler sebagai inisiator data dan Sistem (Platform) sebagai pengolah data.

1. Fungsi Akuisisi Data Sensor (Aktor: Mikrokontroler)

- Mikrokontroler bertindak sebagai aktor utama yang memulai proses pengumpulan data sensor. Fungsionalitas utamanya meliputi:
 - Membaca Sensor RFID: Mikrokontroler mengambil data identifikasi dari modul RFID.
 - Membaca Sensor HCSR-04: Mikrokontroler mengukur jarak menggunakan sensor ultrasonik (HCSR-04).
 - Membaca Sensor Proximity: Fungsi ini di-include ($\llinclude\gg$) oleh kedua pembacaan sensor di atas, mengindikasikan bahwa baik RFID maupun HCSR-04 melibatkan pengukuran keberadaan atau kedekatan sebagai bagian dari operasinya.
 - Ambil Data Di Sensor: Merupakan hasil langsung dari pembacaan *proximity*, yaitu fungsionalitas untuk mengekstrak nilai-nilai terukur dari perangkat keras sensor.
 - Menerima Data Sensor: Fungsi ini di-include ($\llinclude\gg$) oleh *Use Case* Ambil Data Di Sensor, menunjukkan bahwa segera setelah data diekstrak, data tersebut diterima dalam *buffer* sistem untuk diproses lebih lanjut.

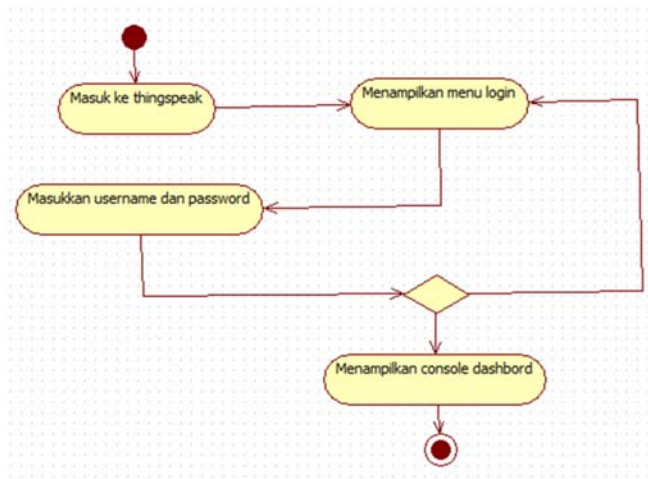
2. Fungsi Pengolahan dan Penyimpanan Data (Aktor: Sistem)

- Sistem (Platform) mengambil alih peran pasca-akuisi data dan bertindak sebagai aktor yang memicu pemrosesan data. Dalam konteks diagram yang dimodifikasi ini, fungsionalitas penyimpanan dan pemrosesan yang sebelumnya dihubungkan ke MySQL dan Mahasiswa dialihkan atau disederhanakan sebagai fungsi internal sistem:
 - Simpan Data: Fungsi ini menjadi *Use Case* krusial yang menerima input dari Menerima Data Sensor dan bertanggung jawab untuk melakukan persistensi data ke media penyimpanan internal sistem atau *database* (implisit) yang dikelola oleh sistem itu sendiri.
 - Hitung Data: Fungsi ini dipicu oleh Sistem dan mengakses data yang telah disimpan (Simpan Data) untuk melakukan analisis, perhitungan, atau validasi yang diperlukan (misalnya, perhitungan rata-rata, konversi unit, atau pemrosesan algoritma).

- Menyimpan Data Sensor: Fungsi ini tidak memiliki aktor eksternal (Mahasiswa) dalam diagram ini, tetapi tetap ada sebagai *Use Case* yang melibatkan Menerima Data Sensor, mengindikasikan bahwa sistem dapat secara otomatis inisiasi proses *Menerima Data Sensor* dan menyimpannya.
- Mengakses Sensor dan Menampilkan Data: Fungsi-fungsi ini sekarang menjadi fungsionalitas internal Sistem, di mana *platform* secara otomatis dapat mengakses data yang telah disimpan (Simpan Data) dan menyediakannya untuk modul tampilan atau *interface* internal (tanpa intervensi eksplisit dari user/siswa).

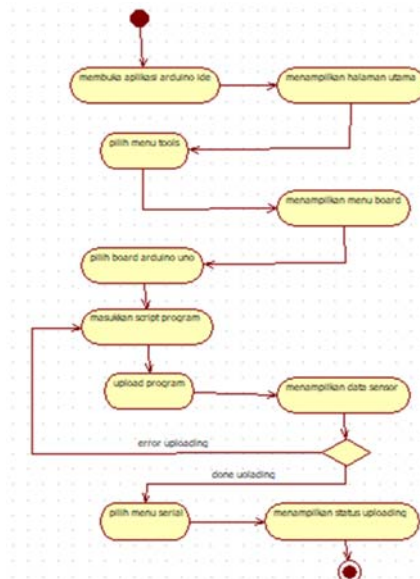
Mikrokontroler memulai siklus dengan membaca berbagai sensor dan mengambil data. Data yang berhasil diambil secara otomatis diterima dan kemudian disimpan oleh fungsi Simpan Data. Data yang telah disimpan ini kemudian digunakan oleh fungsi Hitung Data (dipicu oleh Sistem) dan dapat diakses serta ditampilkan oleh fungsi internal sistem.

3.3. Activity Diagram



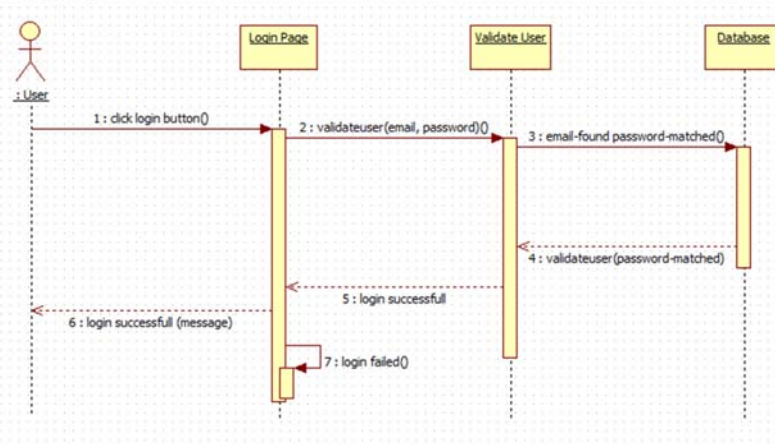
Gambar 3. Activity Diagram Login Platform

Gambar 3. Masuk ke halaman Thingspak, lalu muncul tampilan menu *login*. Masukkan *username* dan *password*. Jika proses *login* berhasil, maka Blynk akan menampilkan menu *dashboard*. Tetapi jika proses *login* tidak berhasil maka kembali lagi ke proses memasukkan *username* dan *password*.



Gambar 4. Activity Diagram Microkontroller

Pada gambar 5. halaman utama di aplikasi Arduino IDE, pilih menu tools lalu cari board arduino uno. Setelah itu, masukan dan upload script program. Jika proses berhasil maka data setiap sensor akan di tampilkan di menu serial monitor, tetapi jika error maka kembali lagi pada prose memasukan dan mengupload script program.

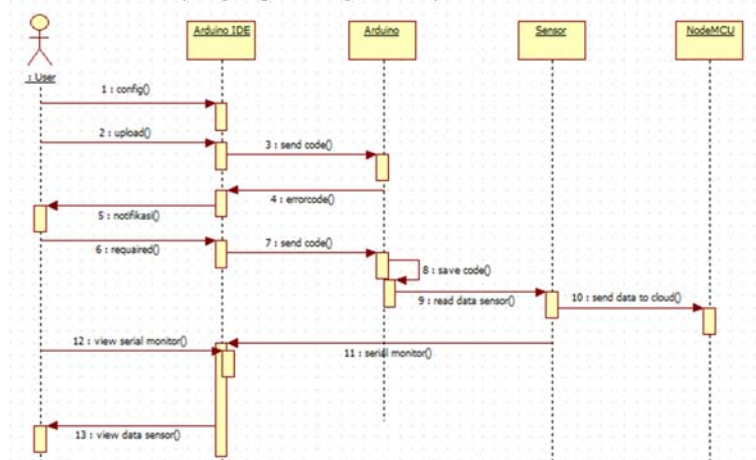


Gambar 5. Sequence Diagram Login Platform

Sequence diagram gambar 5. menggambarkan alur interaksi pengguna dengan sistem pada proses login. Berikut urutan kejadian yang terjadi:

1. Pengguna (User) menekan tombol login pada halaman login (*Login Page*).
2. *Login Page* menerima aksi ini dan mengirim permintaan validasi user ke modul Validate User, dengan menyertakan email dan password yang dimasukkan oleh pengguna.
3. Modul Validate User memeriksa data kredensial pada Database untuk mencocokkan email dan password.
4. Database mengembalikan hasil pencocokan, yang menyatakan apakah password sesuai dengan email yang ditemukan.
5. Jika kredensial valid, modul Validate User mengirimkan notifikasi keberhasilan login (*login successful*) ke *Login Page*.
6. *Login Page* kemudian menampilkan pesan login berhasil kepada pengguna.
7. Jika kredensial tidak valid, *Login Page* menampilkan pesan login gagal (*login failed*).

Diagram ini menunjukkan proses interaksi dasar dalam autentikasi sistem, termasuk pengecekan validitas akun di database dan umpan balik kepada pengguna. Dengan alur ini, sistem memastikan hanya pengguna dengan kredensial sah yang dapat mengakses layanan.

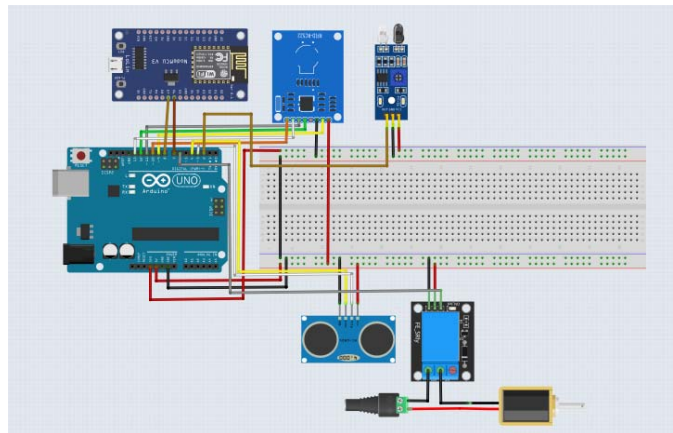


Gambar 6. Sequence Diagram Microkontroller

Sequence diagram gambar 6. menggambarkan alur interaksi antara User, Arduino IDE, Arduino, Sensor, dan NodeMCU dalam sistem monitoring berbasis IoT. Prosesnya dapat dijelaskan sebagai berikut:

1. Konfigurasi Sistem.
 User memulai dengan mengonfigurasi sistem melalui Arduino IDE dengan memanggil fungsi `config()`. Arduino IDE menyiapkan pengaturan awal yang diperlukan untuk komunikasi dengan Arduino.
2. Upload Program ke Arduino.
 Setelah konfigurasi, User melakukan `upload()` program ke Arduino. Arduino IDE mengirimkan kode program ke Arduino (`send code()`), dan Arduino memprosesnya. Jika terdapat kesalahan, Arduino mengirimkan pesan error (`errorcode()`) kembali ke Arduino IDE, yang kemudian menampilkan notifikasi kepada User (`notifikasi()`).
3. Permintaan Kode Tambahan.
 Apabila diperlukan, User dapat melakukan permintaan tambahan melalui fungsi `required()`. Arduino IDE kembali mengirimkan kode ke Arduino (`send code()`) yang selanjutnya disimpan oleh Arduino (`save code()`).
4. Pembacaan Data Sensor.
 Arduino melakukan pembacaan data dari Sensor (`read data sensor()`). Data sensor ini kemudian dikirim ke NodeMCU (`send data to cloud()`) untuk diteruskan ke cloud, memungkinkan monitoring jarak jauh.
5. Monitoring Serial dan Data Sensor.
 User dapat memantau proses melalui serial monitor dengan memanggil `view serial monitor()`. Arduino IDE menerima dan menampilkan data serial dari Arduino (`serial monitor()`). Selain itu, User juga dapat melihat data sensor secara langsung dengan memanggil fungsi `view data sensor()`, sehingga memudahkan pemantauan performa sistem secara real-time.

3.4. Perancangan Alat



Gambar 7. Skema Sistem

Gambar 7. merupakan skema pengkabelan yang penulis buat menggunakan aplikasi *Fritzing*. Dimana pada gambar tersebut terlihat semua sensor terhubung dengan Arduino Uno R3 dan *NodeMcu*. *RFID* memiliki 8 pin namun yang terpakai hanya 7 pin diantaranya VCC terhubung ke daya 3v, GND terhubung ke ground, RST ke pin 9 Arduino, SDA ke pin 10 Arduino, SCK ke pin 13 Arduino, MOSI ke pin 11 Arduino, MISO ke pin 12 Arduino, Sensor IR diantaranya VCC terhubung ke daya 5v, GND terhubung ke ground, pin out ke pin 3. Sensor HSCR ada 4 pin diantaranya VCC terhubung ke daya 5v, GND terhubung ke ground, Relay ada 3 pin diantaranya VCC terhubung ke daya 5v, GND terhubung ke ground pin IN ke pin 6.

Tabel 1 Struktur Tabel Data

No	Atribut	Tipe Data		Keterangan
1	<i>id</i>	<i>Integer</i>	3	<i>Auto Increment</i>

2	RFID	varchar	5
3	Proximity	Float	5
4	HSCR	Float	5
5	Class	Float	50

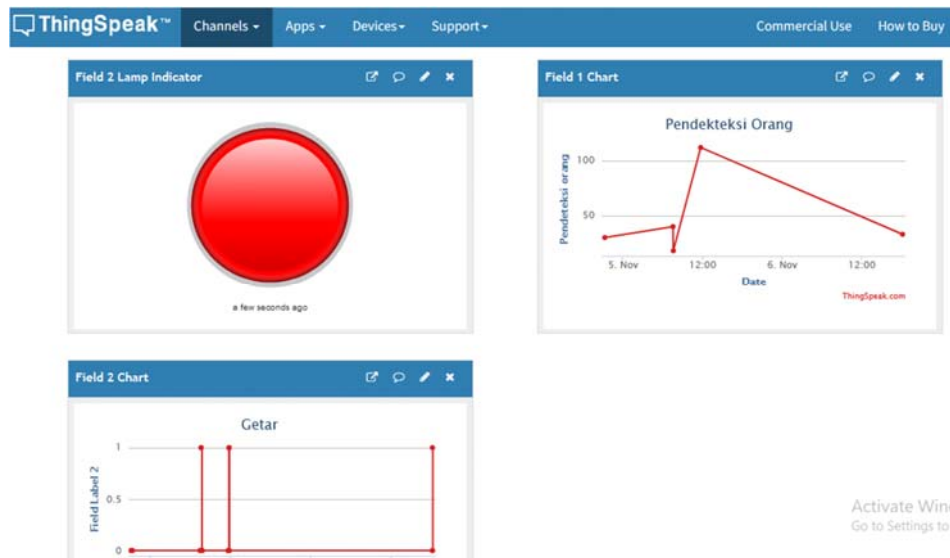
3.5. Implementasi Sistem

Implementasi pengujian alat merupakan gambaran dari pengujian alat yang sudah penulis uji tingkat kelayakan dan tingkat ke akuratannya. Terlihat pada gambar 7.

Gambar 7 menunjukkan tampilan dashboard monitoring berbasis *ThingSpeak* untuk alat yang diuji. Terdapat tiga komponen utama:

1. *Field 2 Lamp Indicator*: Menampilkan indikator lampu berwarna merah yang menyala. Lampu ini menunjukkan status alarm atau peringatan dari alat, menandakan bahwa sistem sedang mendeteksi kondisi tertentu yang memerlukan perhatian.
2. *Field 1 Chart* – Pendeteksi Orang: Grafik ini memvisualisasikan jumlah deteksi orang dari waktu ke waktu. Terlihat bahwa terdapat lonjakan signifikan pada satu titik waktu, menunjukkan bahwa alat mampu mendeteksi kehadiran orang secara akurat dan responsif terhadap perubahan kondisi lingkungan.
3. *Field 2 Chart* – Getar: Grafik ini memperlihatkan aktivitas sensor getar yang dicatat oleh alat. Terdapat beberapa puncak pada grafik, yang menunjukkan bahwa alat berhasil mendeteksi getaran sesuai dengan kejadian yang terjadi. Nilai 1 menandakan terdeteksi adanya getaran, sedangkan nilai 0 menunjukkan tidak ada getaran.

Secara keseluruhan, tampilan dashboard ini memperlihatkan tingkat keakuratan dan responsivitas alat dalam mendeteksi kehadiran orang serta getaran, sekaligus memberikan indikator visual melalui lampu yang menyala untuk kondisi tertentu. Hal ini menunjukkan bahwa alat telah diuji dan siap digunakan dalam pemantauan secara real-time.



Gambar 7 Tampilan Data Pada Platform *Blynk*

Setelah *platform* terkoneksi dengan baik, maka akan diperoleh halaman untuk melakukan proses pendeteksi loker penyimpanan.

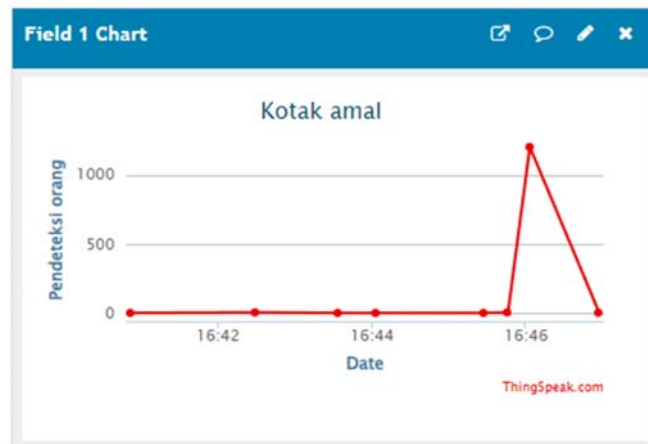
Gambar 8. menampilkan grafik *Field 1 Chart* dari sebuah channel IoT yang memantau aktivitas kotak amal. Sumbu horizontal menunjukkan waktu (Date) dalam format jam dan menit (16:42, 16:44, 16:46), sedangkan sumbu vertikal menunjukkan jumlah pendekat/aktivitas orang dalam satuan orang.

Terlihat bahwa pada interval 16:42 hingga 16:44, jumlah aktivitas sangat rendah, mendekati nol. Namun, pada pukul 16:46 terdapat lonjakan tajam aktivitas hingga mencapai hampir 1000 orang. Setelah lonjakan ini, aktivitas kembali turun drastis ke angka nol. Fenomena ini mengindikasikan bahwa kotak amal mengalami kejadian interaksi signifikan dalam waktu singkat, yang kemungkinan besar terjadi karena seseorang melakukan sumbangan atau sejumlah orang mendekat secara bersamaan.

Grafik ini memberikan informasi penting mengenai frekuensi dan waktu interaksi dengan kotak amal, yang dapat digunakan untuk analisis pola penggunaan serta evaluasi efektivitas penempatan dan desain kotak amal berbasis IoT.

Channel Stats

Created: [2 months ago](#)
Last entry: [less than a minute ago](#)
Entries: 8



Gambar 8 Private View Channel Blynk

3.6. Kesimpulan

Berdasarkan hasil penelitian dan pengujian prototipe kotak amal berbasis Internet of Things (IoT), dapat disimpulkan beberapa hal sebagai berikut:

1. Keberhasilan Perancangan Sistem: Prototipe kotak amal pintar berhasil dirancang menggunakan NodeMCU ESP8266 sebagai pusat kendali, dengan integrasi RFID reader, sensor getar, sensor warna, kunci solenoid, dan relay. Sistem ini mampu memproses data dari sensor secara real-time dan menampilkannya melalui aplikasi Blynk dan platform ThingSpeak.
2. Peningkatan Keamanan dan Transparansi: Sistem yang dikembangkan mampu meningkatkan keamanan kotak amal dibandingkan metode konvensional. Penggunaan sensor getar dan log RFID memungkinkan pemantauan aktivitas kotak secara akurat, sedangkan kunci solenoid mengurangi risiko akses tidak sah.
3. Keakuratan dan Responsivitas: Pengujian alat menunjukkan bahwa kotak amal pintar dapat mendeteksi kehadiran orang dan getaran dengan tingkat akurasi tinggi. Tampilan dashboard menunjukkan indikator visual (lampu) serta grafik aktivitas yang memudahkan monitoring secara real-time.
4. Informasi Analitik: Grafik aktivitas pada Field 1 Chart memberikan data penting mengenai frekuensi interaksi dengan kotak amal, sehingga memungkinkan analisis pola penggunaan dan evaluasi efektivitas penempatan kotak.
5. Potensi Pengembangan Lanjutan: Sistem ini dapat menjadi acuan bagi pengembangan kotak amal berbasis IoT yang lebih kompleks, termasuk integrasi notifikasi otomatis, analisis data lebih lanjut, dan peningkatan fitur keamanan.

Daftar Pustaka

- [1] D. Setiawan and T. Hariono, "Design of a Smart Donation Box Based on IoT," *Newt. Netw. Inf. Technol.*, vol. 3, no. 2, pp. 43–53, Aug. 2024, doi: 10.32764/newton.v3i2.4951.
- [2] Atmiasri, A. Solikin, and A. Puncak Pujiputra, "Implementation of Charity Box Security System based on Internet of Things (IoT) using Sensor and Notifications," *BEST J. Appl. Electr. Sci. Technol.*, vol. 7, no. 1, pp. 7–10, Mar. 2025, doi: 10.36456/best.vol7.no1.10159.
- [3] B. T. Syahputra, "Arduino-Based Anti-Theft System in Mosque Charity Box," *Brill. Res. Artif. Intell.*, vol. 2, no. 3, pp. 81–85, Jun. 2022, doi: 10.47709/brilliance.v2i3.1548.
- [4] Jupriyanto and M. R. Assidiq, "Celengan Pintar Berbasis Iot (Internet Of Things) Menggunakan Platform Blynk Dilengkapi Notifikasi Whatsapp," *Jawara Sist. Inf.*, vol. 2, no. 2, 2025.
- [5] N. Anggraini, Z. Zulkifli, and N. Hakiem, "Development of Smart Charity Box Monitoring Robot in Mosque with Internet of Things and Firebase using Raspberry Pi," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 24, no. 1, pp. 11–24, Nov. 2024, doi: 10.30812/matrik.v24i1.4209.
- [6] D. N. Ilham, R. A. Candra, A. Budiansyah, E. Sipahutar, M. K. Harahap, and F. Anugreni, "Implementation of Vibration Sensor and Pin Lock using Keypad for Charity Box Security," *Int. J. Multidiscip. Sci. Arts*, vol. 1, no. 2, pp. 125–133, Jan. 2023, doi: 10.47709/ijmdsa.v1i2.2050.
- [7] N. Anggraini and M. A. Shaeku, "Implementasi IoT pada Kotak Donasi dengan Sensor TCS3200 untuk Deteksi Uang Kertas Menggunakan Firebase dan Bot Telegram," *J. Inform. Univ. Pamulang*, vol. 9, no. 4, pp. 146–154, Dec. 2024, doi: 10.32493/informatika.v9i4.45280.
- [8] I. F. U. Ma'ruf, Jamaaluddin, and I. Anshory, "Charity Box Based Camera and Security System Internet Of Things and Telegram," *Procedia Eng. Life Sci.*, vol. 3, Feb. 2023, doi: 10.21070/pels.v3i0.1340.
- [9] A. Setiawan, A. I. Purnamasari, N. D. Nuris, I. Ali, and R. Narasati, "IoT: Theft detection of the mosque charity box through Arduino R3 with HC-SR501 sensor and MC-38 sensor," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1088, no. 1, p. 012085, Feb. 2021, doi: 10.1088/1757-899X/1088/1/012085.
- [10] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and L. Castedo, "Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications," Feb. 2024, doi: 10.3390/s17010028.