Indonesian Journal of Artificial Intelligence and Data Mining (IJAIDM)
Vol. 8, No. 2, July 2025, pp. 407 – 416
p-ISSN: 2614-3372 | e-ISSN: 2614-6150

Internet of Things-Based Charity Box Security with Automatic Money Detection and Location Tracking

[1]Nur Septi Anggraini, [2*]Irma Salamah, [3]Aryanti Aryanti
[1,2,3]Telecomunication Engineering, State Polytechnic of Sriwijaya, Indonesia
Email: [1]nurseptiaa15@gmail.com, [2]irma_salamah@polsri.ac.id, [3]aryanti@polsri.ac.id.

Article Info
Article history:
Received May 14th, 2025
Revised Jun 17th, 2025
Accepted Jul 22th, 2025

Keyword:
Charity Box Security
GPS Neo-6M
Internet of Things
TCS3200 Sensor
Telegram Bot

ABSTRACT
This research designs and develops an Internet of Things (IoT)-based charity box security system aimed at improving transparency, security, and efficiency in the management of donation funds. The system integrates a TCS3200 color sensor to detect banknotes, a Neo-6M GPS module for real-time location tracking, and 4x4 keypad as PIN-based access security. The ESP32 microcontroller acts as the control center, and the Telegram Bot API is used to send notifications directly to the user when suspicious activity or device movement occurs. Additional features such as buzzers, speakers, and solenoid doorlocks function as warning systems and automatic locks to prevent unauthorized access. Test results show that all features work well, with a high success rate in money detection, accurate location tracking, and fast notification delivery. Despite limitations in the accuracy of detecting some banknotes due to the similarity of RGB values, the overall system proved to be reliable and has the potential to be implemented in public facilities or places of worship. Further developments could include integration with cloud storage, the addition of cameras for visual identification, and mobile applications for more interactive remote control and monitoring.

Corresponding Author:
Irma Salamah
Telecomunication Engineering,
State Polytechnic of Sriwijaya,
Palembang, South Sumatera, Indonesian.
Email: irma_salamah@polsri.ac.id

DOI: http://dx.doi.org/10.24014/ijaidm.v8i2.37254

1. INTRODUCTION

Charity boxes are one of the main media in collecting funds used to support various social and religious activities, especially in mosques, prayer rooms, foundations, and other public assistance. However, in practice, many charity boxes are targeted for theft or have suspicious funds due to weak monitoring and security systems [1]. Many places of worship still rely on conventional security systems such as ordinary padlocks, without automatic monitoring or alarms [2]. Irregularity in recording and supervision also causes problems in the transparency and accountability aspects of donation management, which can affect public trust [3][4].

As technology advances, Internet of Things (IoT)-based approaches are increasingly being applied in various fields, including security systems. IoT enables data collection from physical sensors that are remotely controlled and monitored via an internet connection [5]. In the context of charity boxes, IoT can be used to connect various security devices such as money detectors, Global Positioning System (GPS) location trackers, authentication keypads, and alarm systems in one integrated platform [6]. With this system, managers can monitor the status and location of the box in real-time, and receive immediate notifications if suspicious activity occurs [7].

Various previous studies have attempted to apply IoT technology to improve the security of donation boxes. Some studies utilize the TCS3200 color sensor to detect the nominal value of money based on the RGB value of the banknotes [8], while other studies develop a location tracking system using the Neo-

6M GPS module that sends coordinates periodically [9]. The use of the Telegram Bot Application Programming Interface (API) is also starting to become popular as a notification medium because it is lightweight, fast, and easy to integrate with microcontrollers [10]. Some studies have even added a 4x4 keypad as a PIN authentication system and a solenoid lock as an automatic lock [11].

However, most of these studies focus on only one or two features, such as money detection or notification systems, and have not fully integrated all security aspects. Not many have integrated money detection, location tracking, authentication systems, sound alarms, and online notifications into a single, integrated system that works simultaneously [12]. Furthermore, existing systems are not equipped with the ability to detect and record unauthorized access attempts, such as Personal Identification Number (PIN) input errors, which risk going undetected by administrators [13].

To address these challenges, this study proposes an IoT-based smart charity box system that integrates five key features: (1) automatic money detection with the TCS3200, (2) real-time location tracking using GPS, (3) a PIN authentication system with a 4x4 keypad, (4) automatic locking with a solenoid, and (5) real-time notification to Telegram in the event of a threat. This system is also equipped with a buzzer and speaker as physical alarms in the event of a break-in or unauthorized access. The system design is made modular and flexible to make it easy to develop, for example by integrating a cloud-based dashboard or indoor tracking based on Wi-Fi and Global System for Mobile Communications (GSM) triangulation [14].

The objective of this research is to design and build an IoT-based donation box security system capable of: (1) Automatically detecting the amount of money, (2) Tracking the location of the box in real time, (3) Detecting suspicious activity such as forced opening or unauthorized movement, (4) Sending notifications directly to the administrator via Telegram, and (5) Providing PIN-based access authentication to prevent unauthorized opening.

To complement the above, the system is also equipped with a speaker and buzzer for audible alerts in the event of forced access or unauthorized activity. The design is built to be modular and flexible, allowing future integration with advanced cloud dashboards, indoor tracking using Wi-Fi Positioning Systems (WPS), or GSM triangulation for enhanced localization accuracy. The main objective of this study is to develop a donation security system that is reliable, cost-effective, and easy to deploy across different institutions. This will contribute to enhancing transparency, reducing fraud, and increasing public confidence in donation management practices.

2. RESEARCH METHOD

2.1. Research framework

The results of the research are displayed in an easy-to-understand and informative way in a visual format. To explain the sequence of tasks performed during the testing phase, block diagrams are very useful. Therefore, the analytical workflow shows the final version of this diagram, which helps to build a well-functioning system. Figure 1 shows the design of the research framework.

This research begins with a literature study to collect references related to IoT-based security systems, money color sensors, 4x4 keypads, and GPS tracking technology. This stage aims to strengthen the theoretical basis that supports system development. Next, system design is carried out, which includes the selection of components and programming of the ESP32 microcontroller to detect the nominal value of money based on color, GPS for location tracking, and verifying the PIN as an access security system. The next stage was hardware and software integration, where all components were assembled and initially tested to ensure that all parts worked synergistically. After that, testing and data collection were carried out through simulations of donation detection, PIN validation, location tracking with GPS, and sending automatic notifications via the Telegram application. The data obtained from this stage is then analyzed to assess the performance of the system and ensure that the designed functionality has run as expected.

2.2. Device Design

The design stage in this research is divided into two main parts: hardware design and software design. The hardware design process begins with creating a complete system block diagram. The tool used is one of the essential components in this diagramming process. Through the block diagram, the overall circuit operation can be visualized and understood. As a result, the block diagram plays a critical role in ensuring the system functions as intended. Block Diagram of Research Framework can view Figure 1.

Based on Figure 2, the block diagram illustrates the overall design of the system. In general, this diagram is divided into three main sections. The first section is the input block that consists of several sensors and input modules, namely the TCS3200 color sensor that functions to detect the color of money, the 4x4 keypad that is used to input codes or commands by the user, the Neo-6M GPS module that provides real-time location data, and the FC-51 sensor that is used to detect the presence of surrounding objects. The second part includes the data processing block performed by the ESP32 microcontroller, known as the ESP32

NodeMCU. This microcontroller serves as the control center of the system and is responsible for reading, processing, and validating the data fed to all the sensors. After processing the data, the ESP32 uses pre-programmed logic to make decisions. The output block, which consists of many components, is in the third section. Such outputs include a door lock solenoid that will open or close according to the amount of data processed, an LCD that displays information to the user, and a Bluetooth speaker that emits voice notifications. To remotely send notifications or information to the user, the system is also connected to Telegram via an ESP32 network connection.

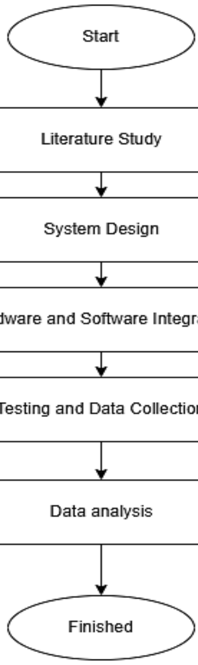

Figure 1. Block Diagram of Research Framework

2.2.1. Hardware Design

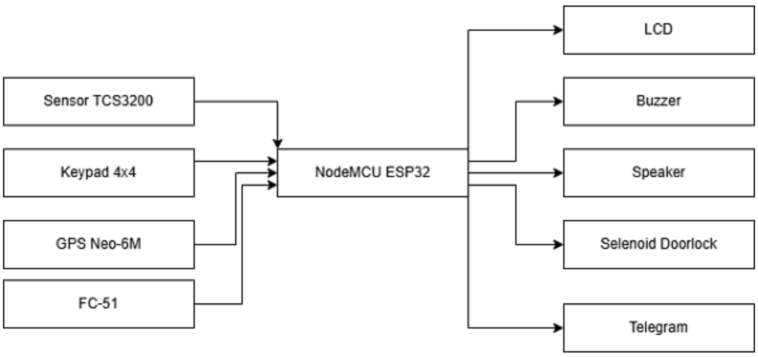

Figure 2. Hardware System Block Diagram

2.2.2. Software Design

The designed software is capable of processing data from the TCS3200 sensor, Neo-6M GPS, infrared sensor (FC-51), and 4x4 keypad based on the protocol of each component. The system uses the ESP32 microcontroller as the controlling center to identify the amount of money, detect the presence of objects around the charity box, verify the user's PIN, and track the location of the charity box directly. Visual information is displayed via LCD, while security alerts are sent via Telegram application. The program creation process is done through the Arduino IDE by utilizing the C++ programming language.

2.3. Flowchart System

Researchers make a system block diagram to facilitate the processing of inputs and outputs from the hardware and software design process that researchers will design. The system flowchart for this study can be seen in Figures 3, 4, and 5.

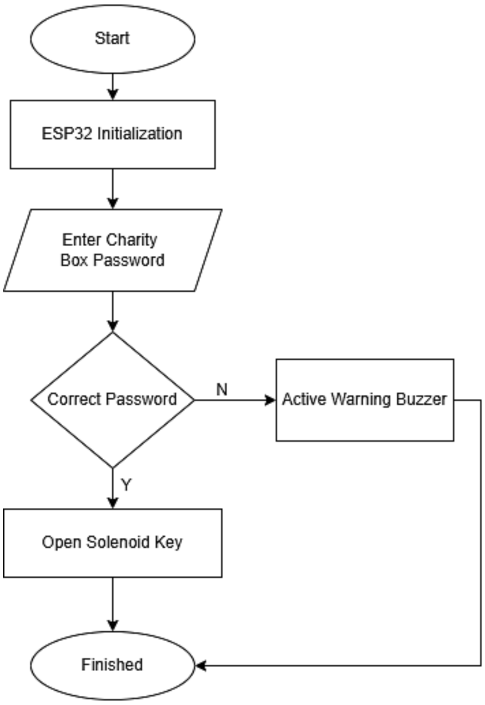

Figure 3. Security System Flowchart

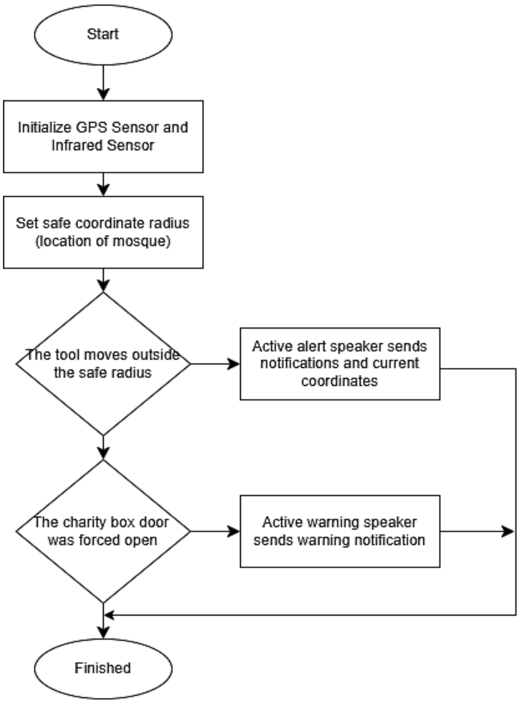

Figure 4. GPS Flowchart

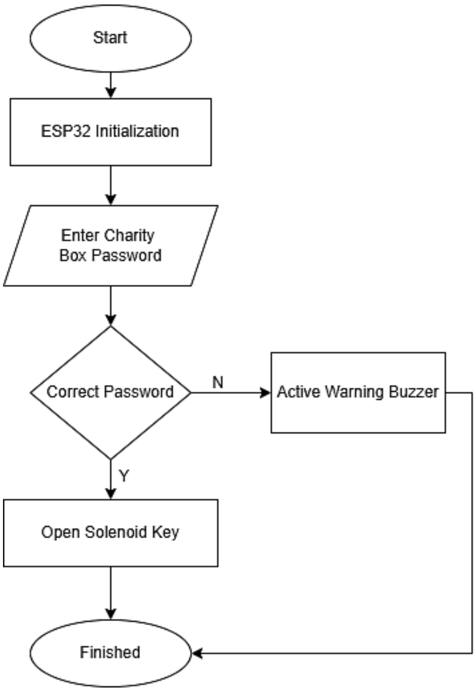

Figure 5. Flowchart of Money Recognition System

2.4. Device Used

2.4.1. Hardware Used

The hardware used in this system includes the NodeMCU ESP32 as the main microcontroller that controls the entire workflow of the system. Other components include the TCS3200 sensor to detect the amount of money, Neo-6M GPS for location tracking, FC-51 IR sensor for motion or object detection, 4x4 keypad as PIN input, LCD as display media, buzzer and speaker as sound alert devices, and solenoid doorlock as a charity box key activator. All these components are connected using jumper cables and work in an integrated manner.

2.4.2. Software Used

The system uses a variety of hardware, with the NodeMCU ESP32 as the main control center that manages all system operations. Among the components used are the TCS3200 sensor to recognize the amount of money, Neo-6M GPS to track the location, FC-51 IR sensor to detect movement or presence of objects, 4x4 keypad as a PIN input tool, LCD to display information, and buzzer and speaker as a sound alert system. In addition, a doorlock solenoid is used as a locking mechanism for the charity box. All these components are interconnected through jumper cables and function in an integrated manner.

2.5. Method development

This system development method involves the process of collecting data from various installed sensors, such as the TCS3200 color sensor, GPS, IR, and keypad. The data obtained will be processed in real-time by the ESP32 microcontroller and sent over the internet network using IoT technology. All of these activities aim to convert raw data into valuable information, such as the amount of money received, the location of the charity box, security status, and access verification. The information is then displayed on the LCD and sent to the user via Telegram as a notification, allowing for efficient and responsive remote monitoring.

2.6. Literature Review

IoT technology is widely used to automate security systems and real-time management of donation boxes. Some commonly used techniques include the TCS3200 color sensor to read currency denominations based on RGB values, the Neo-6M GPS module for position tracking, and the ESP32 as the main microcontroller that manages all data flows [13]. This system is typically enhanced with a 4x4 keypad for user PIN authentication, a speaker and buzzer for audible alerts, and a solenoid door lock for an automatic locking mechanism. This technology enables remote monitoring and automated action upon detection of potential threats.

Several studies have been conducted to develop smart donation box systems using an IoT approach. Automatic money counting systems based on color sensors have become a primary focus of many studies because they can increase transparency in fund management [14]. Furthermore, the use of real-time notifications through applications such as Telegram is a crucial feature for detecting box movement or attempts at unauthorized access [15]. Such systems demonstrate that the integration of sensors and internet-based communication applications can reduce response delays from managers and prevent theft [16][17].

In addition to currency denomination detection and notifications, a physical security system is also crucial in designing a smart donation box. Integration of a PIN keypad and buzzer provides immediate response in the event of an input error, while the use of a solenoid lock keeps the box locked without authorization [18]. Several studies have also developed systems with GPS tracking and vibration detection to ensure the box is not moved unauthorized. However, many systems have not fully integrated all these features into a single platform [19][20]. Most existing solutions suffer from limited scalability and lack a centralized monitoring interface, reducing their effectiveness when deployed at scale or across multiple locations [21]. Some designs focus solely on physical security without incorporating real-time notifications, while others utilize alert systems like Telegram but lack GPS tracking leading to gaps in overall functionality [22][23]. Ideally, a smart donation box should be able to provide a comprehensive solution, from detecting and identifying incoming money, securing physical access, sending instant notifications, remotely tracking locations, and recording usage history for audit purposes [24]. By integrating all of these capabilities into a single, modular, centralized system, transparency, operational efficiency, and reliability in donation box management can be significantly improved [25].

This research aims to fill this gap by combining key features currency denomination detection, PIN authentication, GPS location tracking, audio alerts, and Telegram notifications into a single, integrated and modular IoT system. This system not only improves physical security but also promotes efficiency and accountability in managing the donation box. With this approach, the implementation of smart donation boxes can be more effectively implemented in mosques, social institutions, or other public facilities.

3. RESULTS AND ANALYSIS

This section describes the implementation and testing results of the IoT-based smart charity box system that has been developed. The testing is conducted to ensure that all the main features, such as money detection, PIN security, location tracking, and notification system, work well as expected.

3.1. System Design

System design is the initial stage in the development of an IoT-based smart charity box, which includes integrated hardware and software design. Hardware includes ESP32, TCS3200 sensor, GPS, IR, keypad, LCD, buzzer, speaker, and solenoid. The software is developed using Arduino IDE and integrated with Telegram for notification.

3.1.1. Hardware Design

The system is designed with an ESP32 microcontroller as the control center that connects the various hardware components. These components include a TCS3200 color sensor to detect the amount of money, a 4x4 keypad as input media for PIN verification, an FC-51 infrared sensor to detect objects or movement, and a Neo-6M GPS module to track the location of the charity box. Information is displayed through the LCD screen, while sound alerts are delivered through the buzzer and speaker. The locking mechanism is executed using a solenoid. All these devices are assembled together in one charity box, can see Figure 6 and Figure 7.

Figure 6. Front View of Charity Box

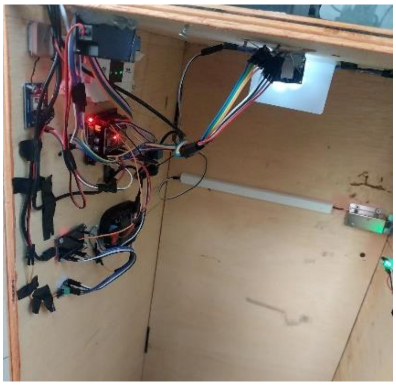

Figure 7. Charity box tool range

3.1.2. Software Design

The system software is developed using the Arduino IDE, which is used to write and upload programs to the ESP32 microcontroller. The program manages the process of reading data from sensors, signal processing, and output control based on specific logic. The system is also integrated with the Telegram Bot API to send real-time notifications to users in the event of suspicious activity, such as the break-in or movement of charity boxes. Serial communication protocol, RGB value reading, and PIN validation are part of the main logic in this software.

3.2. System Security Testing Results

This test is carried out to ensure that only the correct PIN can open the solenoid. The test results were obtained as in the following Table 1.

Table 1. Security System Testing Results

Input	Output		
Password	Selenoid	Buzzer	Speaker
1423	Locked	Active	Active
1330	Locked	Active	Active
1234	Open	Inactive	Inactive
2091	Locked	Active	Active

The results show that the system is able to respond to PIN input accurately, where the solenoid will only open if the PIN entered is correct. In addition, the buzzer and speaker sound that activates when an input error occurs indicates that the warning system is running properly according to its function.

3.3. GPS Location Testing Results

The system was tested by moving the device to determine the accuracy of the GPS sensor. Table 2 shows the coordinate reading results.

Table 2. GPS Reading Results

Experiment	Latitude	Longitude
1.	-2.963658	104.718780
2.	-2.963680	104.718825
3.	-2.963665	104.718775
4.	-2.963665	104.718775

GPS testing showed consistent coordinate readings. The success of the system in tracking the movement of the charity box confirmed the reliability of the Neo-6M GPS module. However, the trials were conducted under ideal environmental conditions with no signal obstructions. In a real implementation indoors or in a densely built-up area, the GPS accuracy may decrease significantly. Therefore, the system can be improved by incorporating other location technologies such as Wi-Fi positioning or GSM triangulation to overcome satellite signal limitations.

3.4. TCS3200 Sensor Testing Results

The TCS3200 color sensor is used to identify banknotes based on RGB values. The results can be seen in Table 3.

Table 3. Money Nominal Testing Results

No	Amount Of Money Tested	RGB Target	Number Of Attempts	Number Of Correct Detections	Success Behavior
1.	Rp1.000	(50,100,50)	10	10	100%
2.	Rp2.000	(170,180,170)	10	7	70%
3.	Rp5.000	(170,170,120)	10	10	100%
4.	Rp10.000	(180,140,200)	10	10	100%
5.	Rp20.000	(130,190,160)	10	7	70%
6.	Rp50.000	(130,180,220)	10	10	100%
7.	Rp100.000	(220,100,120)	10	10	100%

The TCS3200 sensor was able to detect most denominations with a high success rate, except for the IDR 2,000 and IDR 20,000 denominations, which only reached 70%. This is likely due to the similarity of RGB values between certain denominations, as well as variations in lighting during testing. This detection failure risks misclassifying donations and compromising data accuracy. To overcome this, it is possible to recalibrate the sensor based on actual light conditions or use a camera with machine learning-based image processing for more accurate classification.

3.5. Comprehensive System Testing Results

Tests were conducted to determine the system's response to various security scenarios. The results are presented in Table 4.

Table 4. Comprehensive System Testing

No	Scenario	Buzzer	Speaker	Gps	Selenoid	Telegram
1	Charity box forced open	On	On	On	Off	Receives notifications when a charity box is attempted to be forced open and automatically sends the location via telegram
2	Attempted to enter wrong pin password	On	off	Does not provide information on location	Off	Does not receive notifications
3	Charity box moved outside secure radius	On	On	On	Off	Receives notifications when a charity box moves out of radius and the current location can be viewed
4	Entered pin password correctly	Off	Off	Off	On	Does not send messages

The system was tested through various simulated threat scenarios to evaluate the response and performance of each main component, including the buzzer, speaker, GPS, solenoid lock, and Telegram notification system. Below is a detailed explanation of the results presented in Table 4:

1. Charity box forced open
   When the system detected a forced opening attempt, the buzzer and speaker were both activated, providing immediate audio alerts. The GPS module remained active and successfully transmitted the current location. However, the solenoid lock was in the Off state, indicating that the lock had been compromised or bypassed during the attempt. The Telegram Bot functioned as expected, immediately sending a notification to the administrator containing an alert and the GPS coordinates of the box. This scenario validates that the system is capable of detecting unauthorized access and triggering multiple warning mechanisms simultaneously.

2. Attempted to enter wrong PIN password
   In this condition, the system correctly detected invalid PIN input. The buzzer activated as an audible warning, while the speaker remained inactive—suggesting that speaker alerts were only reserved for

more critical security breaches. The GPS module did not activate or transmit any data in this case, which is consistent with the design that only triggers GPS when movement is detected. The solenoid remained locked, as no authorized access was granted. However, the Telegram system failed to deliver a notification, indicating a weakness in the notification logic for failed authentication attempts. This highlights an area for improvement, where failed PIN entries should also be logged and reported for security auditing purposes.

3. Charity box moved outside secure radius
   When the system detected that the charity box was moved beyond the defined secure radius, both the buzzer and speaker were activated to create immediate awareness. The GPS module actively tracked the location and reported it in real-time. The solenoid lock remained in the Off position, signaling the system's intent to restrict access during unauthorized movement. Telegram notifications were successfully sent, including updated location coordinates that could be viewed by the administrator. This confirms that the movement-detection mechanism and location-based alerts were functioning correctly and reliably.

4. Entered PIN password correctly
   In this scenario, the user successfully entered the correct PIN. As expected, all alert components—buzzer, speaker, and GPS—remained in the Off state, indicating that no warning or tracking was triggered because the access was authorized. The solenoid lock was activated (On) to allow access to the donation box contents. The Telegram notification system did not send any messages, which is appropriate behavior, as the system only sends alerts in cases of unauthorized access or abnormal activity. This confirms that the system can distinguish between legitimate and unauthorized access, ensuring that valid users are not unnecessarily alerted or tracked.

The comprehensive system testing demonstrated the effectiveness of the IoT-based charity box in handling various security scenarios. When the box was forcibly opened or moved outside the secure radius, the system responded by activating the buzzer and speaker, tracking the location via GPS, and sending real-time alerts through Telegram. In contrast, during a failed PIN attempt, only the buzzer was triggered, while GPS and Telegram notifications remained inactive—revealing a weakness in the system's ability to log unauthorized access attempts. When the correct PIN was entered, all alert features remained off, and the solenoid lock activated as expected, confirming that the system could differentiate between authorized and unauthorized access. Overall, the system functions well in critical situations, although enhancements are recommended to improve the handling and reporting of failed authentication attempts.

3.6. Telegram App Testing

The Telegram application testing process to ensure the application runs well and has an optimal user experience can be seen in Figures 5 and Figure 6.

Figure 5. Telegram application view

Figure 6. Display charity box notification outside radius

The overall test results show that the system responds well to various security scenarios, such as notifications when the device is moved or forcibly unlocked. However, the consistency of notification delivery was still dependent on network conditions, and there were situations where violations (such as PIN errors) did not result in notifications. This indicates that the functionality of the system is highly affected by the stability of the internet connection.

In general, the test results prove that the system performs according to its original purpose, which is to detect the amount of money, secure access, and track the location with real-time notifications. However, the analysis shows that the system can still be improved, especially in terms of sensor reliability, notification management, and integration of additional technologies to increase accuracy.

3.7. Discussion

The smart donation box system developed in this research demonstrates the superiority of comprehensively integrating various security features. The system combines several critical components, such as currency detection, PIN authentication, location tracking, audible alarms, and real-time notifications, into a single, connected and modular platform. This integration makes the system more responsive to various threats, both physical, such as forced opening, and digital, such as unauthorized access attempts. Test results indicate that the system can perform its functions effectively in several scenarios, such as sending notifications when the box is moved or forced open. However, a weakness was identified in the PIN input error scenario, where the system did not send a notification to the administrator. This indicates a limitation in the notification trigger logic, which is configured to respond only to physical movement, not authentication errors. This situation can result in non-physical burglary attempts going unrecorded, ultimately compromising the overall security level of the system.

This system also has high practical value for implementation in mosques, foundations, or other public facilities that rely on public donations. The modular design allows the system to be tailored to the needs of each location, while the use of popular communication platforms facilitates integration and use without the need for complex additional infrastructure.

4. CONCLUSION

The smart donation box system developed in this research demonstrates the superiority of comprehensively integrating various security features. The system combines several critical components, such as currency detection, PIN authentication, location tracking, audible alarms, and real-time notifications, into a single, connected and modular platform. This integration makes the system more responsive to various threats, both physical, such as forced opening, and digital, such as unauthorized access attempts.

Test results indicate that the system can perform its functions effectively in several scenarios, such as sending notifications when the box is moved or forced open. However, a weakness was identified in the PIN input error scenario, where the system did not send a notification to the administrator. This indicates a limitation in the notification trigger logic, which is configured only to respond to physical movement, not authentication errors. This situation can result in non-physical burglary attempts going unrecorded, ultimately compromising the overall security level of the system.

This system also has high practical value for implementation in mosques, foundations, or other public facilities that rely on public donations. The modular design allows the system to be tailored to the needs of each location, while the use of popular communication platforms facilitates integration and use without the need for complex additional infrastructure.

REFERENCES

[1] N. I. Qalbi, C. W. Purnama, N. I. Dwi, A. B. Kaswar, and J. M. Parenreng, "Rancang Bangun Kotak Amal Cerdas," *J. Media Elektr.*, vol. 17, no. 2, pp. 25–32, 2020, doi: 10.59562/metrik.v17i2.14034.

[2] N. Anggraini, Z. Zulkifli, and N. Hakiem, "Smart Charity Box Monitoring with IoT," *Matrik J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 24, no. 1, pp. 11–24, 2024, doi: 10.30812/matrik.v24i1.613.

[3] N. Azizah, F. C. Chasanah, W. E. Nugroho, and P. Wibowo, "Rancang Bangun Sistem Monitoring Uang Kertas Berbasis Android," vol. 1, no. 2, pp. 116–123, 2023, doi: 10.52330/jmeis.v1i2.177.

[4] F. C. Furqonie, A. Z. Hasibuan, and A. Sembiring, "Rancang Bangun Kotak Penyimpanan Uang Berbasis Mikrokontroller," *Algoritm. J. Ilmu Komput. dan Inform.*, vol. 7, no. 2, pp. 1–11, 2024, doi: 10.30829/algoritma.v7i2.15718.

[5] F. Yasharsujud, I. Ruslianto, and . S., "Sistem Keamanan Kotak Amal Berbasis Internet of Things (Iot)," *Coding J. Komput. dan Apl.*, vol. 11, no. 1, p. 51, 2023, doi: 10.26418/coding.v11i1.58035.

[6] H. Hamrul, N. Rasyid, Suhardi, and Sakaria, "Perancangan Sistem Keamanan Kotak Amal Berbasis Internet of Things," *Pros. Semin. Nas. Pemanfaat. Sains Dan Teknol. Inf. 2023*, vol. 1, no. 1, pp. 33–40, 2023.

[7] 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, 2023, doi: 10.47709/ijmdsa.v1i2.2050.

[8] I. A. Syahruli, J. Prayudha, and M. Ramadhan, "Penghitung Uang Otomatis dengan TCS3200," *JURSIK TGD*, vol. 1, no. 5, pp. 168–178, 2022, doi: 10.53513/jursik.v1i5.5692.

[9] M. Ramadhan and R. Prayoga, "Integrasi GPS Neo-6M dalam IoT Donasi," *J. Elektron. dan Kendali*, vol. 6, no. 1, pp. 35–42, 2023.

[10] R. Amalia and D. Febrian, "Notifikasi Real-Time dengan Telegram Bot," *J. Elektron. dan Kendali*, vol. 5, no. 2, pp. 55–62, 2022.

[11] I. F. U. Ma'ruf, M. Hidayat, and R. A. Putra, "Pengamanan Kotak Amal Berbasis Telegram," *J. Teknol. dan Sist. Komput.*, vol. 5, no. 1, pp. 44–48, 2022.
[12] A. Hasrudianto, "Rancang Bangun Sistem Penghitung Jumlah Uang Kertas Berbasis Arduino Uno," *J. Mosfet*, vol. 2, no. 1, pp. 15–19, 2022, doi: 10.31850/jmosfet.v2i1.1571.
[13] D. Meilantika and A. Sembiring, "Telegram Notification pada Sistem Keamanan Kotak Amal," *J. Sist. Inf. dan Apl.*, vol. 7, no. 1, pp. 70–78, 2023.
[14] S. Lestari, B. Wijaya, and T. Rahman, "GSM Triangulation untuk Lokasi Perangkat Bergerak," *J. Komputasi Cerdas*, vol. 3, no. 3, pp. 150–159, 2022, doi: 10.1007/s00521-022-07000-1.
[15] H. Gushardi and D. Faiza, "Perancangan dan Pembuatan Alat Penghitung Jumlah Uang Otomatis Terintegrasi IoT," *J. Pendidik. Tambusai*, vol. 6, no. 1, pp. 2996–3005, 2022.
[16] Y. Lavanya, K. Vishnukanth, B. Bhanuprasad, B. Naresh, and M. Divakar, "IoT based Anti–Theft System for Enhanced Protection," *Int. J. Eng. Res. Adv. Technol.*, vol. 10, no. 3, pp. 22–26, 2024, doi: 10.31695/IJERAT.2024.3.3.
[17] D. Gupta, I. Srivastava, S. Verma, G. Saraswat, S. Mishra, and R. Agarwal, "IoT–Based Laser Anti–Theft Security System with Telegram and Gmail Alert," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 14, pp. 349–351, 2023, doi: 10.48175/IJARSCT-10850.
[18] A. B. Kaswar and J. M. Parenreng, "Penggunaan Sensor TCS3200 untuk Pengenalan Uang Otomatis pada Sistem IoT," *J. Teknol. Inf. dan Komput.*, vol. 5, no. 2, pp. 22–28, 2022.
[19] G. Gunawan, A. Yani, Junaidi, Zumhari, E. Hutajulu, and R. Sirait, "Design and Development of a Vehicle Security System Using Vibration Sensors and GPS Based on Arduino," *J. Inf. Technol. Comput. Sci. Electr. Eng.*, vol. 1, no. 3, p. 152, 2023, doi: 10.61306/jitcse.v1i3.152.
[20] IOT-Enhanced Vehicle Security and Recovery System Team, "IOT-Enhanced Vehicle Security and Recovery System," 2023.
[21] P. S. Abarna, Vishal, and others, "IoT Integrated Smart Donation Box," in *Ramsita 2025*, Atlantis Press, 2025. doi: 10.2991/978-94-6463-716-8_52.
[22] N. A. Zuhriyah and S. Rosyadi, "Smart Charity Box with ESP32 and Chatbot," *J. Robot. Autom. Electron. Eng.*, vol. 2, no. 2, pp. 87–99, 2024, doi: 10.21831/jraee.v2i2.613.
[23] I. F. U. Ma'ruf and Jamaaluddin, "Sistem Kamera dan Pengamanan Kotak Amal Berbasis IoT dan Telegram," *Procedia Eng. Life Sci.*, vol. 3, no. 0, p. 1340, 2024, doi: 10.21070/pels.v3i0.1340.
[24] B. T. Syahputra, "Arduino-Based Anti-Theft System in Mosque Charity Box," *Brill. Res. Artif. Intell.*, vol. 2, no. 3, p. 1548, 2024, doi: 10.47709/brilliance.v2i3.1548.
[25] Atlantis Press, "IoT Integrated Smart Donation Box: ensuring efficiency and transparency in charity automation," in *Proceedings of RAMSITA 2025*, Atlantis Press, 2025, pp. 699–706. doi: 10.2991/978-94-6463-716-8_52.

BIBLIOGRAPHY OF AUTHORS

Nur Septi Anggraini, was born in Palembang on September 15, 2003. Currently the author is a final semester student in the Telecommunication Engineering Study Program, Electrical Engineering Department, Sriwijaya State Polytechnic

Dr. Irma Salamah, S.T., M.T.I., currently serves as a lecturer in the Telecommunication Engineering Study Program, Electrical Engineering Department, Politeknik Negeri Sriwijaya. She completed her undergraduate education (S1) at Sriwijaya University in 2002, then earned a master's degree (S2) from the University of Indonesia in 2011, and continued her doctoral studies at Persada Indonesia University Y.A.I. until she graduated in 2023. In the academic field, he has produced a number of scientific works, one of which is entitled Designing a Remote Smart Home Monitoring System Using the Internet of Things (IoT) published in 2022.

Aryanti, S.T., M.Kom., currently serves as a lecturer in the Telecommunication Engineering Study Program, Department of Electrical Engineering, Sriwijaya State Polytechnic. She completed her undergraduate education (S1) at Sriwijaya University in 2002, then continued her master's studies (S2) at one of the universities in Indonesia. Aryanti has produced a number of publications, one of which is entitled Motion Graphic Production Design for Lake Shuji Lembak Tourism Promotion Video which was published in the Proceedings of the 2024 International Seminar.