Quick Response Anti-Theft Measures in Jewelry Stores and Banks Utilizing the Internet of Things

Sarono Widodo[1], Hutama Arif Bramantyo[2], Endro Wasito[3], Muhammad Daffa[4], Lutfi Yuliana[5], Eni Dwi Wardihani[6], Taufiq Yulianto[7], Helmy[8]

[1,2,3,4,5,6,7,8] *Telecommunication Engineering, Department of Electrical Engineering, Politeknik Negeri Semarang, Semarang, Indonesia*

Abstract— The act of theft is a prevalent criminal activity within society, particularly observed in financial institutions and jewelry establishments, owing to the significant economic worth associated with valuable assets like currency, gold, and diamonds. Certain locations lack an integrated security system that interfaces with law enforcement, hence posing challenges for victims to report criminal incidents, particularly in cases involving armed or violent attackers. Hence, the purpose of this final project tool is to streamline and expedite theft reporting by leveraging the capabilities of the Internet of Things. This tool gathers empirical data in the form of visual representations, geographical coordinates, and temporal information pertaining to an incident. The development process employs the waterfall methodology, characterized by an average data transmission speed of 21.5 seconds and a database-to-telegram latency time of around 3.85 seconds. The complete duration encompassing the stages of detection and subsequent notification via telegram amounts to approximately 25.35 seconds. The test results indicate a location tolerance of around 5-10 meters relative to the test spot.

Keywords— Theft, Touch Sensor, IPCam, ESP32, Internet Of Things.

1. Introduction

Crimes, such as theft, are prevalent and pose a significant threat to individuals' lives, possessions, and reputations. The Indonesian Central Statistics Agency reported that theft offenses constituted the second-highest occurrence rate among criminal activities between 2018-2020, with 71,524 recorded [1]. Banks and jewelry shops are particularly susceptible to theft due to their economic value and involvement in financial transactions and trade of valuable commodities. However, many lack robust security systems linked with law enforcement agencies.

The Internet of Things (IoT) has the potential to enhance security measures in the banking and jewelry industries. By leveraging IoT technology, a robust and streamlined security system can be established to safeguard against theft incidents, minimizing potential losses in both sectors. This project aims to develop a security system called "Quick Response Anti-Theft Measures in Jewellery Stores and Banks Based on the Internet of Things."

The proposed system uses a touch detection tool to enhance functionality, allowing the human hand to serve as an interface for transmitting commands to a tool for efficient communication of crime-related information. The system also uses the internet network to communicate with the police, who use a monitoring website to retrieve and display data pertaining to theft instances.

The system will also transmit informative messages, including taken photographs, location coordinates, time of occurrence, and Google Maps data, all provided through the Telegram program. Telegram is used for its low compression, preserving the original quality of images, and the open-source Application Programming Interface (API) technology allows developers to create Telegram bots [2].

This research uses various periodicals as sources of reference. The first article [3] discusses the design and construction of an automated street light monitoring system using an ESP32 microcontroller and Telegram Bot API, which is widely considered an acceptable option for developing IoT applications due to its integrated Bluetooth and Wi-Fi capabilities. The second article [4] discusses the use of microcontrollers for IoT-based home security systems with telegram notifications, which are used to disseminate information upon successful detection of movement by the sensor.

The third article [5] presents a motorcycle security system with a microcontroller-based GPS tracker and Android application, which incorporates a GPS module to transmit precise coordinates of the integrated motorized vehicle to the owner's smartphone. The fourth article [6] introduces an automatic room lock system using NFC technology and touch sensors, which serves as a contingency system in case of malfunctions encountered by the primary access system. The fifth article [7] presents a web-based home security system with an SMS gateway, which includes multiple sensors, including PIR, temperature, and IPcam sensors, to enhance security within the immediate vicinity.

The sixth article [8] proposes the development of an IP camera-based environmental security system using Wi-Fi technology, which is designed to enhance the efficiency and automation of incident reporting in high-value establishments like jewelry stores and banks. The system uses IoT technology to facilitate the prompt dissemination of information regarding theft occurrences, with a rapid reaction mechanism using a touch sensor to promptly dispatch a telegraph notification to law enforcement authorities in case of ongoing criminal activity. The instrument is also integrated with a criminal monitoring feature that provides information on instances of theft, which can be accessed through the provided website.

2. Method

In broad terms, a system constructed utilizing the waterfall methodology is a structured approach employed to strategize, gather, scrutinize, and display data with the aim of achieving a predetermined research target. The fabrication of this rapid response tool can be broadly categorized into three components: hardware design and manufacturing, software development, and mechanical design. The software development process involves the utilization of programming tools such as Arduino IDE, VSCode, and Eagle. The hardware aspect involves the design of a collection of components, tools, and a microcontroller.

2.1. Hardware Planning

The touch sensor employed in hardware design is the TTP223 module. The TTP223 Touch Sensor module is an electrical device designed for the purpose of detecting physical touch on its surface. The present module utilizes capacitive technology for the purpose of detecting alterations in capacitance upon touch, afterwards transforming this information into a digital signal that can be effectively employed across a diverse range of electronic applications. The additional components consist of the ESP32 microprocessor and the Neo 6M GPS module. The ESP32 serves as a data processor acquired from the sensor touch module, and subsequently transmits the data from the IPCam to the database over a WiFi network. The following is a comprehensive overview of the network system.

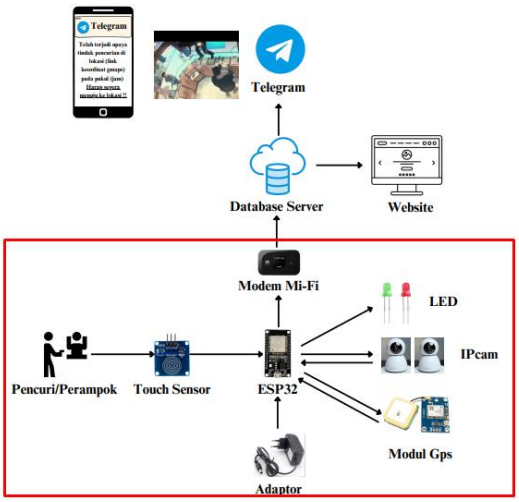

Figure 1. General Architecture

Figure 1 displays a single touch sensor. The touch sensor will perform hand-touch detection which will then be transmitted and processed by the ESP32. The sensor data received by the ESP32 will undergo processing in order to generate a command that will result in the activation of the LED, causing it to emit a green light. Furthermore, the ESP32 device is capable of acquiring image capture outcomes from an IP camera, as well as gathering position data from a GPS module. These capture results, together with the corresponding location coordinates, are then transmitted to a web server for storage in a database. Based on its technical specs, the ESP32 is outfitted with Wi-Fi and Bluetooth modules that enable data transmission over wired or wireless means, utilizing an internet connection. The provided image depicts the comprehensive hardware design.

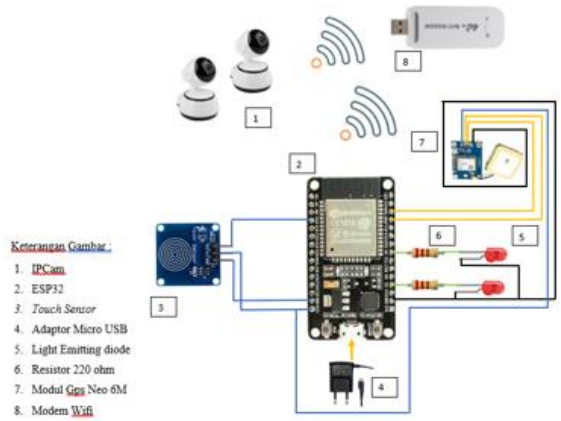

Figure 2. Overall Hardware Planning

Figure 2 depicts a hardware architecture comprising multiple components and sensors that are regulated by an ESP32. Each of the aforementioned components and sensors is equipped with a touch sensor for the purpose of detecting the presence of hand touch. An IPcam is utilized to capture images of theft events, while a Neo 6M GPS module is employed to provide location point information. Additionally, an LED serves as an ESP32 marker that is connected to the Internet, and it also functions as a signal indicating when the touch sensor has been touched. The output data will undergo processing on the ESP32 device before being transmitted and stored in the database. The hardware wiring configuration is as follows.

Input / Output		Mikrokontroller	Keterangan
Touch Sensor	SIG	Pin GPIO 13	Input pin GPIO 13
	VCC	Pin Vin (5V)	Input Tegangan 5V
	GND	Pin GND	Tersambung dengan ground
Resistor 220 Ω	Kaki resistor	Pin GPIO 26	Dihubungkan dengan kaki anoda led merah
Resistor 220 Ω	Kaki resistor	Pin GPIO 12	Dihubungkan dengan kaki anoda led hijau
LED Merah	Anoda (+)	Pin GPIO 26	Penyambungan dari resistor 220 Ω
	Katoda (-)	Pin GND	Tersambung dengan ground
LED Hijau	Anoda (+)	Pin GPIO 12	Penyambungan dari resistor 220 Ω
	Katoda (-)	Pin GND	Tersambung dengan ground
Modul GPS Neo 6M	VCC	Pin Vin (3v3)	Input tegangan 3.3V
	RX	Pin GPIO 16	Input pin RX
	TX	Pin GPIO 17	Input pin TX
	GND	Pin GND	Tersambung dengan ground

Figure 3. Hardware Cable

Figure 3 depicts the utilization of a single ESP32 microcontroller, which receives a voltage input from an

adapter via a micro USB connection with a 30-pin output capacity. The hardware wiring for this design commences with connecting a touch sensor, which consists of three pins (SIG, VCC, and GND), to the corresponding pins on the ESP32 microcontroller. Specifically, the VCC pin of the touch sensor is connected to the Vin (5V) port on the microcontroller, the SIG pin is attached to GPIO 13, and the GND pin is connected to the GND pin on the microcontroller. Subsequently, the 220 Ω resistor is linked to GPIO 26 and GPIO 12 pins, facilitating its connection to the anode (+) of the LED. The cathode (-) of the LED is then connected to the GNC pins on the ESP32. Subsequently, the Neo 6M GPS Module is equipped with four pins, namely VCC, RX, TX, and GND, serving certain functions. The VCCs of each of these pins are attached to the 3V3 pins, the RX GPS is connected to GPIO 16 pins, the TX GPS is connected to GPIO 17, and the GND GPS is connected to the GND pin.

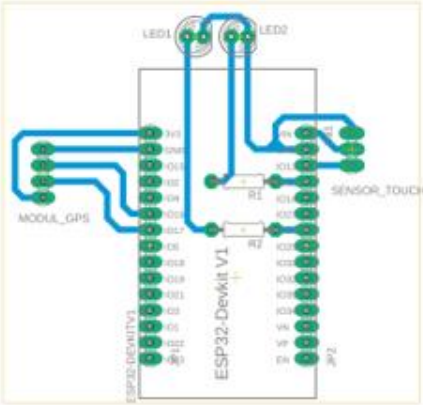

Figure 4. PCB Image Layout

Figure 4 depicts a schematic representation of the proposed arrangement for the printed circuit board (PCB) tracks. This procedure is executed subsequent to the finalization of the hardware wiring design. The connection of the cable table to the ESP32 is crucial for achieving a reliable and organized network output. Subsequently, the grid lines shall be imprinted into the printed circuit board (PCB) in accordance with the specified dimensions.

2.2. Software Planning

Flow diagrams were created for the software design in order to illustrate the algorithm system and its quick response anti-theft operations. The schematic representation of the flow diagram is depicted in Figure 5.

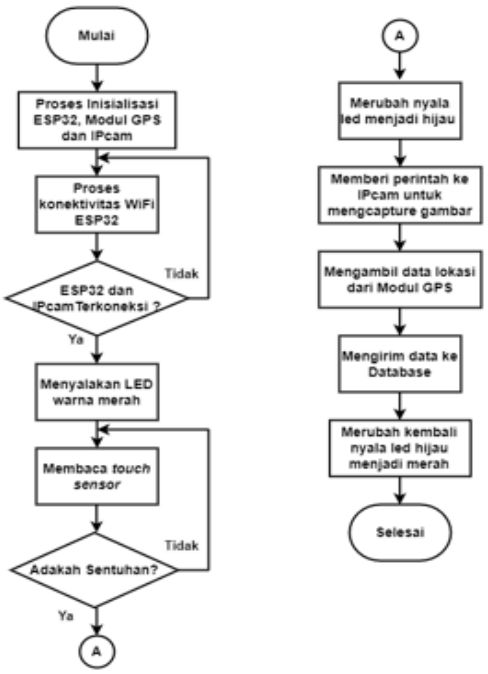

Figure 5 illustrates the flowchart for the design of the system algorithm.

Figure 5 depicts a flowchart illustrating the sequential progression of the system design, commencing with the ESP32 program startup process and subsequently transitioning to the establishment of Wi-Fi network connectivity on the system. In the event of a failed network connection, the ESP32 will persistently attempt to establish connectivity. Subsequently, upon the successful establishment of a Wi-Fi connection, the ESP32 microcontroller will activate the red light-emitting diode (LED).

The aforementioned procedure entails the utilization of a touch sensor to perceive the occurrence of a tactile interaction. When a touch is detected, the corresponding data will be assigned a value of "1" or HIGH. Conversely, in the absence of contact, the data will be assigned a value of "0" or LOW. In the event that the data possesses a low value, the system will persist in its reading of the touch sensor. In the event that the data possesses a significant value, it will be transmitted by the sensor to the ESP32 microcontroller for the purpose of regulating the LED light. The ESP32 device will additionally engage in data processing in order to transmit orders to an IP camera that is linked to the same Wi-Fi network. The ESP32 microcontroller will additionally remain in a state of readiness to receive location information from the GPS module.

The GPS module operates by receiving a radio signal emitted by a satellite, which transmits location data in the form of coordinates. The LED indicator on the GPS Module serves as a visual representation of the module's current state. An LED that does not blink signifies that the module is in the process of searching for satellites in order to carry out a position point computation. When the light-emitting diode (LED) consistently flashes at a frequency of one hertz,

it indicates that a module has effectively acquired a signal from a satellite and determined the position point. Once the IPcam and GPS Module have effectively completed their respective tasks, the collected data will be transmitted to the ESP32 for storage in the database. This transmission will occur through the web server, utilizing the pre-existing Mi-Fi Internet network.

In order to differentiate the position specifics of individual devices, it is proposed to develop a location encoding system that utilizes binary code for storage within the database. The purpose of this identification is to determine the precise location of the device's installation.

Kode Unit Layanan	Polsek Terdekat
001	Polsek Tembalang
010	Polsek Banyumanik
011	Polsek Semarang Selatan
100	Polsek Pedurungan
101	Polsek Candisari

Kode Lokasi	Keterangan	Kode Keseluruhan
0000 0001	Bank BRI Tembalang	001 0000 0001
0000 0010	Bank Mandiri Undip Tembalang	001 0000 0010
0000 0011	Bank Jateng Polines Tembalang	001 0000 0011
0000 0100	Bank BTN Tembalang	001 0000 0100
0000 0101	Toko Emas Semar Nusantara Banyumanik	010 0000 0101
0000 0110	Toko Emas Mustika Banyumanik	010 0000 0110
0000 0111	Bank BNI Banyumanik	010 0000 0111
0000 1000	Bank Mandiri Banyumanik	010 0000 1000
0000 1001	Toko Emas Sumber Mas	011 0000 1001
0000 1010	Toko Perhiasan Tanjung Mas	011 0000 1010
0000 1011	Bank BRI UNIT Mrican	011 0000 1011
0000 1100	Bank Jateng KC Semarang	011 0000 1100
0000 1101	Toko Sumber Mas Tlogosari	100 0000 1101
0000 1110	Toko Emas Bagong	100 0000 1110
0000 1111	Bank BRI UNIT Pedurungan	100 0000 1111

2.3. Mechanical Design

This stage involves the implementation of the devices and components that have been previously prepared. During the mechanical planning phase of tool fabrication, several sequential activities need to be undertaken, specifically:

2.3.1. Devices Preparation.
The tool is manufactured using several devices and components, including an ESP32 microcontroller, two IPcams, a GPS module, two LEDs, two 220 Ω resistors, and an adapter for providing voltage to the ESP32.

2.3.2. Installation of Components

Kode Lokasi	Keterangan	Kode Keseluruhan
0001 0000	Bank Jateng KCP Majapahit	100 0001 0000
0001 0001	Spilla Jewelry Semarang	101 0001 0001
0001 0010	Bank Mandiri KCP Semarang Patrajasa	101 0001 0010
0001 0011	Bank Sinarmas Syariah	101 0001 0011
0001 0100	Bank Neo Commerce	101 0001 0100

Figure 6 the description of location data is provided.

The database design process will involve the utilization of the Entity Relationship Diagram (ERD) technique, as described in the location data description provided in Figure 6. The Entity-Relationship Diagram (ERD) is a widely employed technique in the development of information systems. It serves as a fundamental tool for designing a cohesive and interconnected system by representing and elucidating the interconnections between databases. These relationships are established based on the inherent connections or associations between the fundamental data elements.

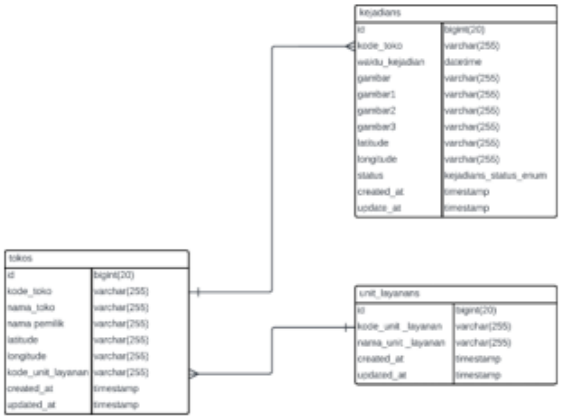

Figure 7 depicts an Entity Relationship Diagram.

According to Figure 7, there exists a mutual relationship among three interconnected tables, namely tokos, kejadians, and layanans units. The website-based monitoring system exhibits a one-to-many relationship between the tables, namely between the "tokos" table and other tables.

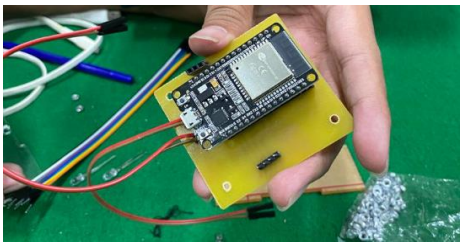

Figure 5. Component Installation Accident

As seen in Figure 8, The installation process commences with the assembly of the ESP32 component, which is affixed onto the completed printed circuit board (PCB). The 220 Ω resistor, which has been previously prepared, is mounted on the PCBA board through a hole. During the assembly process, the GPS module is affixed to the wall of the tool box, specifically within a pre-prepared hollow. Subsequently, the LED installation method involves placing

the LED on the top surface of the toolbox. The wiring assembly throughout the tool's production process is calibrated to conform with the pre-established wiring design. During the installation phase, the touch sensor is connected by means of a tape cable that is safeguarded by a spiral cable. The cable spiral serves the dual purpose of safeguarding the cable and facilitating a seamless installation process.

2.3.3. Installation of IP Cameras

In order to facilitate the installation of an IP camera, it is necessary to supply electrical power to the device by connecting it to a voltage source. This can be achieved by utilizing an adapter and a USB cable specifically designed for the IP camera. The installation process of an IP camera, as depicted in Figure 9.

Figure 6. IPcam Installation

3. Result and Discussion

Following a sequence of design iterations and manufacturing processes, the resultant quick reaction tool assumes the form seen in Figure 11.

Figure 8. Tool Making Results

The tool is installed on the prototype by placing it at the bottom of the table, which has been appropriately equipped with a socket. The tool box contains many components, including the ESP32 microcontroller, the GPS module, a resistor, and an LED. Two poles have been installed, each equipped with two IP cameras positioned at their respective ends. The pillar is depicted as a vertical structural element resembling a solid barrier within an enclosed space. Subsequently, a cable spiral is affixed to the base of the desk and subsequently linked to the lid of the aperture on the table. The cable spirals consist of tape cables that establish a

2.3.4. Prototyping

Prototyping is a crucial stage in the product development process. It involves creating a preliminary version of a product to test its functionality,

This phase entails the realization of a physical representation of a gadget, sometimes referred to as a prototype, which accurately embodies its intended design and functionality. The prototype for this system was constructed using a study table and a pillar as supporting means. The table can be compared to the office table at a bank teller or a jewelry store, while the pillar can be likened to a wall within a room. In Figure 10, the process of prototyping is depicted.

Figure 7. Prototyping

connection between the touch sensors located on the cable line cover and the tool boxes positioned beneath the table. Presented here is Figure 12, which illustrates the physical configuration during the installation of the tool onto the prototype.

Figure 9. Install Tool on Prototipe.

Upon the completion of the installation process, the subsequent stage will involve the evaluation of the acquired data results obtained from a series of tests conducted on the designed and manufactured systems in this final task. This evaluation will encompass the retrieval of data pertaining to the device's performance, as well as the collection of data to ascertain the speed of data transmission from the device to the database. Additionally, location data will be gathered to assess the device's accuracy in detecting specific locations. The data obtained from the test will be carefully monitored and evaluated in order to make meaningful conclusions and provide appropriate recommendations.

3.1. Tool Performance Testing

In order to conduct performance testing, the device will undergo a simulation of a theft event to assess the quick response device's capability to detect any type of contact. In this experiment, an observation is conducted to assess the likelihood of encountering errors throughout the ongoing test. The output of the tool yields a visual representation of theft data on a website called "Simotian.info" as well as a group on the Telegram application titled "Samotian". The experimental setup for tool performance testing is depicted in Figure 13.

Figure 13 Set Up Tool Performance Testing

Figure 13 depicts the configuration of the instrument employed in the performance evaluation of the aforementioned tool. The examination is conducted through the meticulous arrangement of requisite instruments and equipment, followed by the execution of a simulated theft scenario. Once all the devices receive electrical voltage. The initial step of this examination will involve conducting a verification of the Wi-Fi connectivity on the ESP32, IPcam, and Laptop devices. The verification of the ESP32 connection is denoted by the activation of a red light-emitting diode (LED), which serves the dual purpose of illuminating and signifying the device's standby mode.

Subsequently, the assessment of laptop and IP camera connectivity can be accomplished through the process of scanning the respective IP addresses assigned to each device. Once all devices have been successfully linked to the Wi-Fi network, the subsequent step involves monitoring the GPS Module. If the GPS module effectively acquires a sufficient number of signals, it will exhibit a blinking pattern occurring at regular intervals of 1 second. Nevertheless, in the event that an adequate signal strength is not attained, GPS modules will fail to provide a blinking signal. Figure 14 illustrates the successful transmission and reception of satellite signals using GPS modules. The successful connection of the GPS module is depicted in Figure 14.

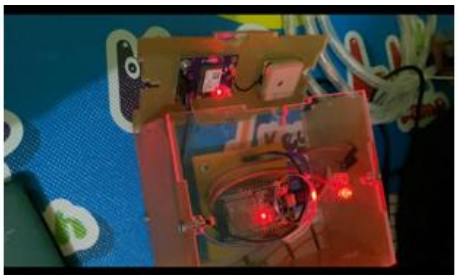

Figure 14. GPS module successfully connected

Once all the necessary checks have been completed, the subsequent step involves initiating the simulation by activating the touch sensor that has been in a standby condition. Once the touch sensor embedded in the quick response device registers a tactile input, the red LED will be deactivated and subsequently replaced by the activation of the green LED. The touch sensor depicted in Figure 15 has been activated through physical contact.

Figure 15. Touch Sensor has been touched

Figure 15 illustrates that when the green LED is in the active state, it indicates the ongoing data transmission process initiated by the image capture, time, and location point. This process involves the ESP32 device, which is responsible for processing the data and subsequently uploading it to the designated database. Upon the completion of the data transfer procedure, the green LED will be deactivated while the red LED will be reactivated. In order to ensure accurate data entry into the database, it is possible to conduct a verification process using phpMyAdmin on the structure u1568590_simotian, specifically on the event table. Figure 16 illustrates the successful integration of the data into the database. In Figure 16, the process of verifying the integrity and accuracy of a database is depicted.

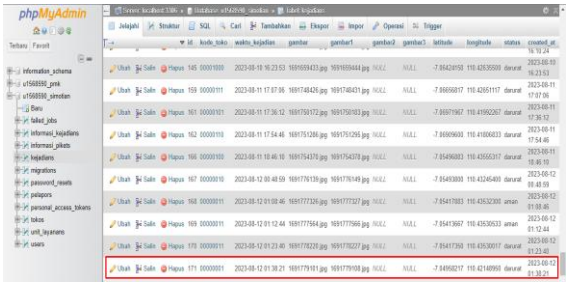

Figure 16. Checking on Database

After the verification of the data in the database, the subsequent task involves ensuring its visibility on the

designated website, namely by conducting a thorough examination of the website titled "Simotian.info". The data will be shown on the website inside the event map menu, providing details regarding the occurrence of the stolen activity. Figure 17 illustrates the presence of the data on the webpage. In this section, we present Figure 17, which depicts the Simotian Web Event Map and Data Checking.

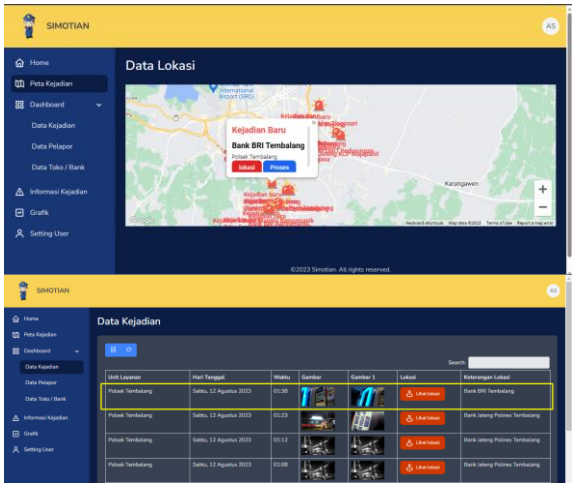

Figure 17 Simotian Web Event Map and Data Checking

Lastly, it is imperative to verify that the data has been recorded within the messaging platform known as "Simotian" on the Telegram application. Figure 18 illustrates the successful input of data into the telegrams application. In accordance with Figure 18, a verification process was conducted via the messaging application Telegram.

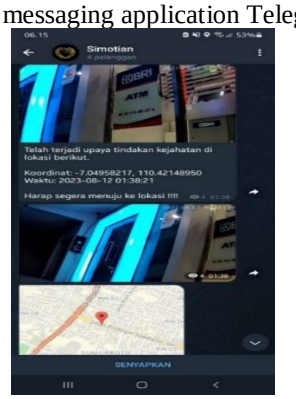

Figure 18. Check on Telegram.

3.2. Tool Performance Testing Without a GPS Module

This tool can be utilized independently of the GPS Module by modifications made in the coding settings of the ESP32 microcontroller. These modifications involve the inclusion of certain commands pertaining to the longitude and latitude coordinates of a given place. The inclusion of these coordinate coordinates is necessary to ascertain the precise location and orientation of the rapid response tool. The experiment involves deactivating the GPS module on the quick response device by disconnecting one of the cords linked to the VCC. The subsequent information pertains to Figure 19, which illustrates the non-utilization of the GPS module. The disabling of the GPS module is depicted in Figure 19.

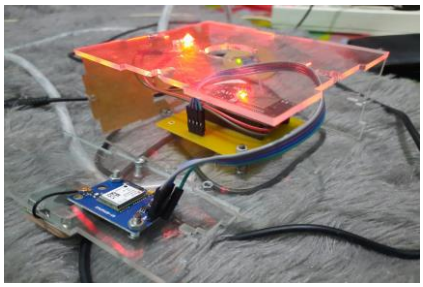

Figure 10. GPS Module Disabling

After the removal of the GPS module, the subsequent step involves uploading the program to the modified ESP32 device at the part pertaining to latitude and longitude coordinate points. The following examples illustrate this process:

The variable "lat" is a character pointer that stores the value "-7.051582".

The variable "lng" is assigned the value "110.426416" as a character pointer.

Subsequently, proceed with the activation of the program designated for the GPS module. Presented above is a visual representation, in the form of a picture denoted as "20," illustrating the outcomes derived from the aforementioned test. Figure 20 displays the results obtained without the utilization of a GPS module.

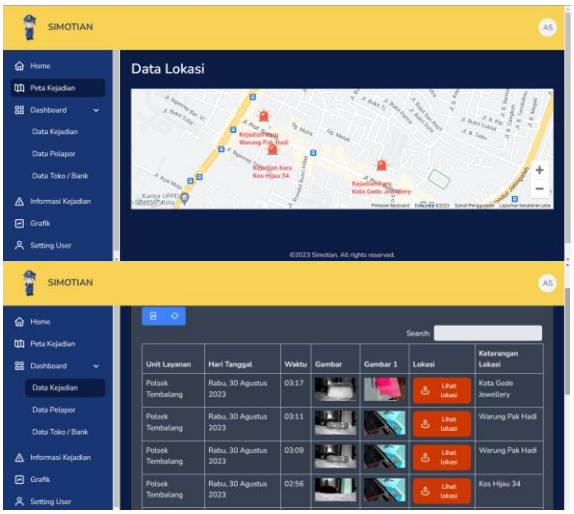

Figure 11. View Results Without GPS Module

After the transmission of information data to the website, the same information will be sent through the messaging feature of the Telegram program. In Figure 21, the results of the Telegram View are presented in the absence of a GPS module.

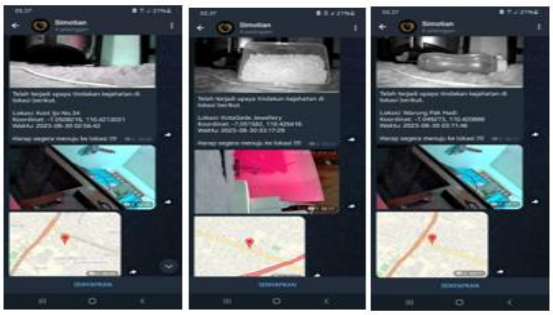

Figure 12. Telegram View Results without GPS Module

This observation suggests that the quick response tool can effectively operate without the need for a GPS module. The ESP32 microcontroller has been programmed to include a feature that allows for the encoding of the position of a store or rapid response device depending on its coordinate point.

3.3. Data Delivery Speed Test

Adjacent to this subsequent examination lies the metric of data transmission velocity, sometimes referred to as response time. The response time test involves measuring the duration it takes for the data to be transmitted from the touch sensor to the database. The objective of this reaction time assessment is to ascertain the speed at which data is provided to law enforcement authorities during emergency situations. The data transfer speed was evaluated by utilizing the time.is website as a reference point to determine the exact moment when the touch sensor was activated. Presented in Figure 22 is an image depicting a website with a real-time clock, alongside a comparative evaluation of its quick response tool in relation to the time.is website. In this study, the researchers conducted response time testing, as depicted in Figure 22.

Figure 22. Response Time Testing

A total of 20 trials were conducted for the quick-response test. The database allows for the observation of data submissions that have been deemed successful. The diagram presented in Figure 23 visually demonstrate the successful input of the data illustrates the Data Delivery Checker.

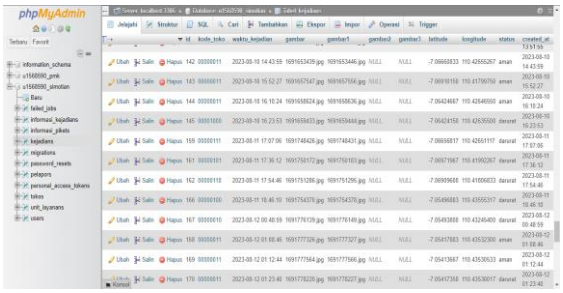

Figure 23. Data Delivery Checker

To determine the speed at which the quick response tool transmits message information, one can compare the timestamp recorded by the touch sensor with the timestamp recorded in the database. This can be achieved by utilizing the website time.is to accurately synchronize the time data. Subsequently, a computation will be performed to determine the temporal disparity necessary for the device to transmit the data to the database. The following analysis presents a comparison of the data depicted in Figure 24, which is provided below.

No	Waktu sensor saat disentuh	Waktu data terkirim pada database	Terdeteksi Sentuhan	Waktu yang diperlukan
1.	01:38:12 WIB	01:38:28 WIB	Terdeteksi	16 detik
2.	00:48:50 WIB	00:49:09 WIB	Terdeteksi	19 detik
3.	01:23:30 WIB	01:23:48 WIB	Terdeteksi	18 detik
4.	18:46:00 WIB	18:46:18 WIB	Terdeteksi	18 detik
5.	17:36:03 WIB	17:36:23 WIB	Terdeteksi	20 detik
6.	17:54:35 WIB	17:54:55 WIB	Terdeteksi	20 detik
7.	17:07:00 WIB	17:07:11 WIB	Terdeteksi	11 detik
8.	16:23:43 WIB	16:24:04 WIB	Terdeteksi	21 detik
9.	14:42:30 WIB	14:42:49 WIB	Terdeteksi	19 detik
10.	13:42:21 WIB	13:42:42 WIB	Terdeteksi	21 detik
11.	15:09:52 WIB	15:10:37 WIB	Terdeteksi	45 detik
12.	16:28:17 WIB	16:28:41 WIB	Terdeteksi	24 detik
13.	17:47:33 WIB	17:47:46 WIB	Terdeteksi	13 detik
14.	17:40:12 WIB	17:40:28 WIB	Terdeteksi	16 detik
15.	18:09:29 WIB	18:09:46 WIB	Terdeteksi	17 detik
16.	18:18:22 WIB	18:18:40 WIB	Terdeteksi	20 detik
17.	13:23:20 WIB	13:23:43 WIB	Terdeteksi	23 detik
18.	12:31:54 WIB	12:32:17 WIB	Terdeteksi	23 detik
19.	13:06:48 WIB	13:07:17 WIB	Terdeteksi	25 detik
20.	12:56:01 WIB	12:56:24 WIB	Terdeteksi	23 detik
Rata-rata waktu				21.5 detik

Figure 24. Data Delivery Speed Test Results

Based on the visual representation provided, it can be observed that there exists a disparity between the time at which the sensor is touched and the corresponding data transmission to the database, as presented in the tabular format. The average duration for data delivery is calculated to be approximately 21.5 seconds. This finding suggests that the implementation of the prompt response mechanism has effectively facilitated the swift transmission of data, thereby

minimizing the occurrence of data theft within a timeframe of less than one minute. Furthermore, it is worth noting that the test findings can be visually represented through the utilization of graphical illustrations, as exemplified in Figure 25.

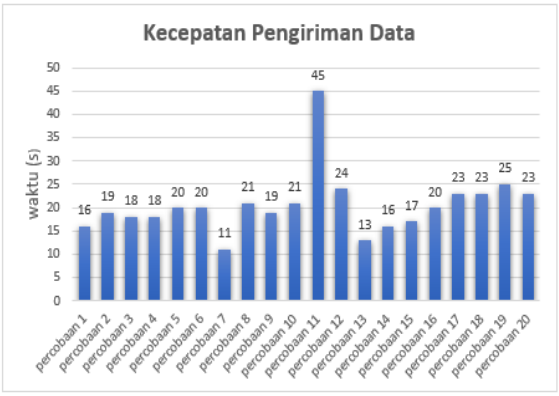

Figure 25. Data Delivery Speed Graph

Furthermore, the evaluation encompasses the measurement of the rate at which data is transmitted from the device to the database. During this phase, we also evaluate the duration of data delay from the database in order to generate a notification on the Telegram platform.

No	Waktu data terkirim pada database	Waktu muncul notifikasi telegram	Waktu yang diperlukan
1.	01:38:28 WIB	01:38:32 WIB	4 detik
2.	00:49:09 WIB	00:49:12 WIB	3 detik
3.	01:23:48 WIB	01:23:51 WIB	3 detik
4.	18:46:18 WIB	18:46:21 WIB	3 detik
5.	17:36:23 WIB	17:36:27 WIB	4 detik
6.	17:54:55 WIB	17:54:58 WIB	3 detik
7.	17:07:11 WIB	17:07:14 WIB	3 detik
8.	16:24:04 WIB	16:24:06 WIB	2 detik
9.	14:42:49 WIB	14:42:53 WIB	4 detik
10.	13:42:42 WIB	13:42:47 WIB	5 detik
11.	15:10:37 WIB	15:10:50 WIB	13 detik
12.	16:28:41 WIB	16:28:41 WIB	4 detik
13.	17:47:46 WIB	17:47:46 WIB	4 detik
14.	17:40:28 WIB	17:40:31 WIB	3 detik
15.	18:09:46 WIB	18:09:49 WIB	3 detik
16.	18:18:40 WIB	18:18:43 WIB	3 detik
17.	13:23:43 WIB	13:23:48 WIB	5 detik
18.	12:32:17 WIB	12:32:23 WIB	6 detik
19.	13:07:17 WIB	13:07:17 WIB	0 detik
20.	12:56:24 WIB	12:56:26 WIB	2 detik
Waktu rata-rata			3.85 detik

Figure 26. Delay Time Test Results

According to the data presented in Figure 26, the average duration for testing the time delay of data transmission from the database to the inclusion of information in a telegraph notification message is 3.85 seconds.

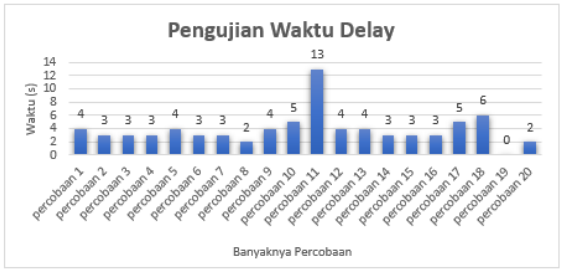

Figure 27. Delay Time Test Graph

Figure 27 displays the graph representing the delay time test. The initial test yielded an average data transmission speed of 21.5 seconds. In the subsequent test, the recorded duration for data delay time to the telegram database was 3.85 seconds. Hence, the cumulative duration required for the device to register a tactile input and transmit a message to a telegraph notification system amounted *to 25.35 seconds.*

3.4. Position Point Accuracy Test

At this juncture, the examination of this particular site can be categorized into two distinct components:

3.4.1. Evaluation of GPS Module via Position Testing

During this step of location testing, the program script's location code is modified for each try. Each test involves relocating the tool placement to a distinct location based on the location data description stored in the database. The examination will assess the accuracy of location data acquired through the rapid response tool by analyzing the obtained results. Figure 28 illustrates the inclusion of location data on the event map presented on the website.

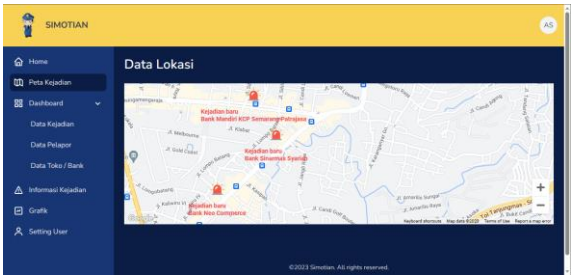

Figure 13. Position map testing with GPS module

Figure 29 illustrates the location outcome conveyed through a telegraph message notice, wherein the device layout and location code are differentiated.

Figure 14. Location Results on Telegram Notifications

By analyzing images 28 and 29, obtained from the event map on the Simotian website and notifications received through the Telegram platform, one can assess the reliability of the provided information by cross-referencing it with the Google Maps program.

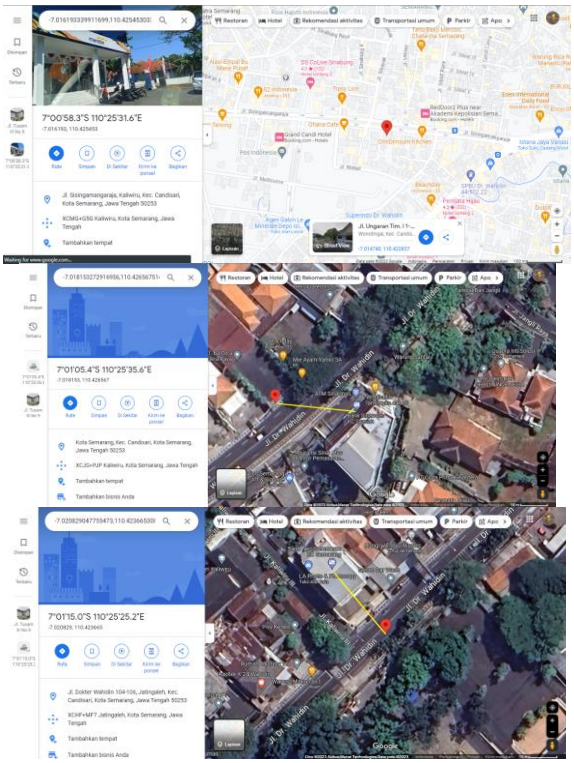

Figure 15. Verification Results via Gmaps

Based on the provided image depicting the outcomes of the location test, it can be observed that the quick response tool has effectively transmitted the location data in the form of coordinate points, as well as facilitated the sharing of location information through both a website and the messaging platform Telegram. Nevertheless, there exists a permissible margin of error in the range of approximately 5 to 10 meters when determining the accuracy of the acquired findings in relation to the test site of the device and its corresponding geographical coordinates.

3.4.2. Conducting Position Accuracy Testing in the Absence of a GPS Module

In order to verify the position without utilizing the GPS module, the procedure involves deactivating the GPS Module program and substituting it with a manual configuration to input a coordinate point into the program encoding residing in the ESP32 microcontroller. The results received from the test are presented in Figure 31.

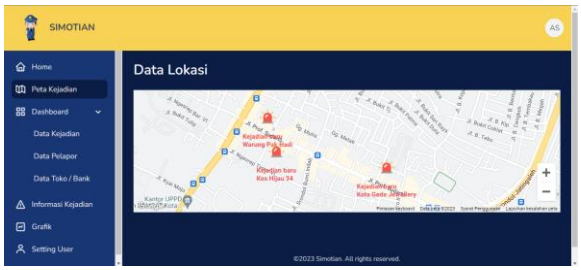

Figure 16. Position map results without GPS module on website

The image provided yields a highly favorable outcome in terms of precise location accuracy. This finding aligns with the location data received through the "SIMOTIAN" group on the Telegram application. I am interested in obtaining a more comprehensive analysis of the geolocation information that has been successfully obtained for the image. The results of location accuracy, as depicted in Figure 32, are presented in the absence of a GPS module.

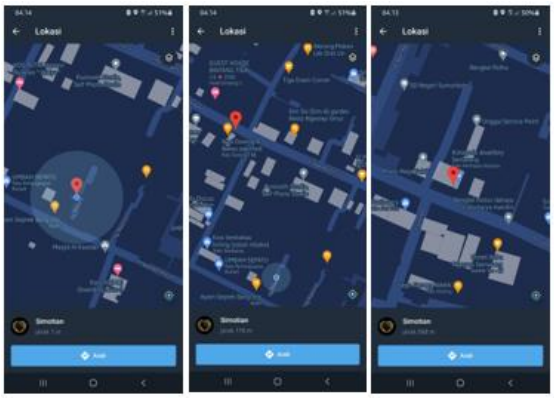

Figure 17. Location Accuracy Results Without GPS Module

4. Conclusion

The comprehensive process of planning, manufacturing, and testing the end task, dubbed "Quick Response Anti-Theft Action in Banks and Internet of Things-based Jewelry Stores," can be summarized as follows: The evaluation of this rapid response tool demonstrates its ability to promptly provide information regarding theft incidents, including captured images as proof, descriptions of the area, coordinates, time, and the option to share the location using Google Maps. The duration of the data transmission speed test, measured from the moment the sensor detects a touch to the time it is received and transmitted as a telegraph notification message, is recorded as 25.35 seconds. The

device's location accuracy test yielded a tolerance range of around 5-10 meters between the test point and the actual location on the site.This technology can be characterized as a rapid response tool due to its ability to transmit emergency information signals to the police in under one minute.

The success of testing without the utilization of GPS modules is attributed to its ability to generate precise location points and coordinates without any margin of error, unlike when GPS modules are employed. The present quick response tool possesses potential for further development in order to enhance its functionality and maximize its benefits. Hence, the further recommendations for the advancement of this tool are as follows: In a subsequent phase of advancement, the tool has the potential to incorporate a nocturnal motion detection camera. The utilization of a GPS module warrants reevaluation, since its deployment should be limited to objects or entities that are mobile and undergo spatial displacement.

References

[1] Central Bureau of Statistics. 2021. *CRIMINAL STATISTICS 2021*. Catalog: 4401002. Jakarta: Central Statistics Agency.

Dickson Kho. 2021. "Understanding Resistors and their Types." Electrical engineering.

[2] Lenardo, Gilang Citra, and Yuda Irawan. 2020. "Utilization of Telegram Bots as Academic Information Media at STMIK Hang Tuah Pekanbaru." *JTIM: Journal of Information Technology and Multimedia* 1(4): 351–57.

[3] Yazid, Yusril Athallah Muhammad, and Rizqi Agung Permana. 2022. "Design of Automatic Street Light Monitoring Prototype Using ESP32 Microcontroller and Telegram Bot Api." *Journal of Informatics Engineering* 8(1): 12–19.

[4] Ratnasari, Fitria, Prahenusa Wahyu Ciptadi, and R Hafid Hardyanto. 2021. "IoT-Based Home Security System Using Microcontrollers and Telegram As Notifications." In the Proceedings Series of the National Seminar on Informatics Dynamics,

[5] Mahaputra, I Gusti Agung Made Yoga, I G A Putu Raka Agung, and Lie Jasa. 2019. "Design and Build a Motorcycle Security System Using a Microcontroller Based GPS Tracker and Android Application." *Electrical Technology Scientific Magazine* 18(3): 361–68.

[6] Permana, Fajar Surya, Sony Sumaryo, and I G Prasetya Dwi Wibawa. 2018. "Implementation of an Automatic Room Lock System Based on Near Field Communication Technology and Touch Sensors." *eProceedings of Engineering* 5(3).

[7] Hamidi, Eki Ahmad Zaki, Mufid Ridlo Effendi, and M Rizki Ramdani. 2020. "Web-Based Home Security System Prototype and SMS Gateway." *TELKA-Journal of Telecommunications, Electronics, Computing and Control* 6(1): 56–65.

[8] Sarjanoko, Raden Joko. 2022. "Design and Build a Wifi-Based Environmental Security System Using an Ip Camera." *TeknoIS: Scientific Journal of Information Technology and Science* 12(1): 79–84.

[9[Isnaini, Vandri Ahmad, Rahmi Putri Wirman, and Indrawata Wardhana. 2015. "Characteristics and Efficiency of Light Emitting Diode (LED) Lamps as Energy Saving Lamps." *Pros. Semin. Nas. MIPA and Pendidik. MIPA* 1: 135–42.

[10] Satyadji, Abimanyu, Aji Gautama Putrada, and Rizka Reza Pahlevi. 2021. "Analysis of the Influence of Perceived Usefulness and Perceived Ease of Use Factors on the Acceptance of Smart IP Camera Users in the Waiting Room of the Setabelan Community Health Center, Surakarta." *eProceedings of Engineering* 8(5).

[11] Yudhanto, Yudho, and Abdul Azis. 2019. *Introduction to Internet of Things Technology (IoT)*. UNSPress.

[12]Zul, Muhammad Ihsan, Lukito Edi Nugroho Widyawan, and L Nugroho. 2012. "Motion Detection Using the Frame Differences Method on an IP Camera." *Proceeding CITEE 2012*: 52–56.

[13] Muliadi, Muliadi, Al Imran, and Muh Rasul. 2020. "Smart bin development using esp32." *Electric Media Journal* 17(2): 73–79.

[14] Pressman, Roger S. 2012. "Software engineering: a practitioner's approach."