ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse222952020.pdf
https://doi.org/10.30534/ijatcse/2020/222952020

Enabling of Technology in Preventing Vandalism in Tower Communication

Hidayat[1], Suryadiputra Liawatimena[2]
[1] Computer Science Department BINUS Graduate Program - Master of Computer Science, Bina Nusantara University Jakarta, Indonesia 11480,hidayat001@binus.ac.id / hidayat.nompo@gmail.com
[2]AComputer Science Department BINUS Graduate Program - Master of Computer Science Bina Nusantara University
Jakarta, Indonesia 11480. Computer Engineering Department Faculty of Engineering Bina Nusantara University, Jakarta, Indonesia 11480, suryadi@binus.edu / s.liawatimena.id@ieee.org

ABSTRACT

The theft of telecommunication tower supporting devices or commonly known as Base Transceiver Station (BTS), continues to increase every year, as reported by digital media viva.co.id from several operators who stated that they found significant losses from the theft. Reported by the daily Republika.co.id, in 2013, Telkomsel operators claimed to have lost up to Three billion rupiahs more due to the theft of BTS batteries in only a few districts and cities in South Sulawesi. Therefore it is necessary to evaluate the method of using technology to prevent damage. The vandalism prevention system can design by utilizing the Internet of Things (IoT) technology. The design uses a Raspberry Pi computing module, which is accompanied by a GSM transmission module to send a response signal to the motion captured by the camera. Photos are sent to the server, in this case, the Telegram Bot

Key words : Vandalism, Anti-Theft Technology, Tower communication, Object detection, IoT

1 INTRODUCTION

The operator has reported the theft to the police. They also invited the surrounding community to socialize the benefits of a communication tower and invited the community to take care of maintaining BTS facilities by increasing security coordination with the authorities if there is potential for vandalism. The operator has also submitted an increase in theft cases to the regulator (Ministry of Communication and Information) of the Republic of Indonesia government.

To note, theft and destruction of telecommunications infrastructure violate article 36 of the Criminal Code. Besides, there is also Law No. 36 about a very worrying situation. Moreover, similar incidents continue to occur this year, allegedly going to increase every year in line with the growth of telecommunications tower construction in Indonesia. The growth of telecommunication towers, both owned by tower operators and providers, as shown in Figures 1 and 2, is growing fast but is not yet accompanied by effective preventive solutions to reduce vandalism occurrence.

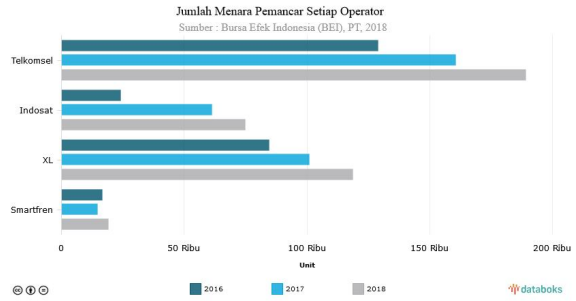

Figure 1. Number of transmitter towers per operator (Dwi, 2018)

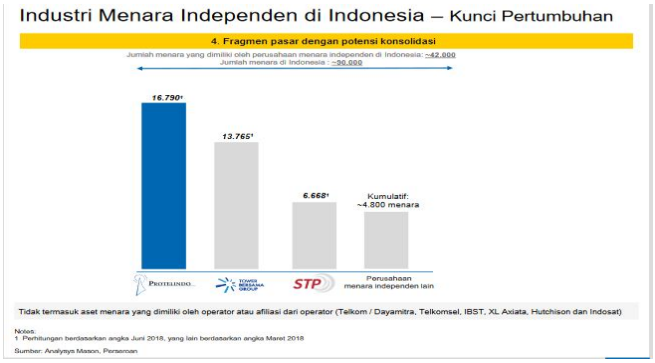

Figure 2. Independent tower industry in Indonesia (Rivan, 2018)

To prevent and even anticipate vandalism, the operator has formed a task force internally and even cooperates with the authorities. However, the destruction still occurred because a special task force and the apparatus were not around BTS hours. Closed Circuit Television (CCTV) technology solutions have also been implemented in several central BTS.

However, they are considered inefficient to be implemented in hundreds of thousands of telecommunications towers. In addition to the high price of implementation, it also requires a large bandwidth to transmit data to the server. However, the conventional equipment lock has two potential problems: vandalism and counterfeiting. To fulfil the control and track the potential illegal behaviour, the human labour and paper are required to proceed with related operations, resulting in the consumption of a large amount of human resources and maintenance costs [34]

Internet of Things (IoT) is a trend and innovation that is used by almost all industries throughout the world. The Internet of Things refers to objects that can be uniquely identified as virtual representations in Internet-based structures. The term Internet of Things was initially suggested by Kevin Ashton in 1999 and gained prominence through the Auto-ID Center at MIT. And now, the IoT is one of the assignments for a student in a college. The most important features of IoT include artificial intelligence, connectivity, sensors, active involvement, and the use of small devices.

The advantages of IoT can be applied in the vandalism prevention system in the communication tower. Does not require high implementation and operational costs, and can be useful and fast in prevention. Therefore this research uses the approach of IoT technology in finding solutions to achieve research objectives.

2 RELATED WORKS

Cases of communication device vandalism have occurred since the early emergence of cell phone technology. However, studies related to cases that explain communication towers as objects of destruction from my search are not available. However, similar cases can be used, especially for the topics of anti-theft technology, human object detection, camera surveillance, and security monitoring systems.

In a review of research related to anti-theft technology, some of which can be used as a guide in research. The study [3] uses a cable electronic detection module Voltage detection is used to detect cable theft, which detects voltage battery as a measuring voltage. The vehicle's engine cranking system is secured by interfacing the Arduino UNO board, fingerprint sensor, and relay, which collectively forms the anti-theft system and provides better protection from unauthorized persons [6].

The proposed RFID-based anti-theft system is capable of detecting movement of the asset that attached to the RFID tag. The design of the motion-sensitive RFID tag with interrupt function is capable of sending the motion alert signal to the reader in real-time [6]. The study [21] revealed that the RFID System has a limited recognition range, which helps protect stolen cultural objects and respond to the alarm on time.

From the approach of several previous studies found several methods in implementing a security system, including: The research [1] focuses on the main objective of the proposed design is to improve the security system by minimizing costs and increasing security capabilities.

Research [7] develops Geospatial Sensor Observation Services for can align diverse sensor networks, support heterogeneous sensor data storage, and meet individual requirements. Different users are a big challenge. This paper proposes a Service-oriented framework for integrating and assimilating sensors observations and measurements under the multi-purpose SOS in combination with other standard services_CSW, WFS-T, and WCS-T.

A study [11] proposes that USCS is controlled by the Remote network based on UPnP. The OSGi platform is used to expand UPnP and provide a remote control for home-based IP cameras via a network controller. The proposed system makes it possible for users to monitor the status of the home for property security, to care for parents or children, and as a protection against accidents, research [36] uses Xively and Twitter's tools to filter process conditions sent from controllers and update the same directly to vehicle owners. which is considered more effective and quicker in delivering information for prevention

Many previous studies recommend Passive Infra-Red (PIR) sensors to detect human objects with the consideration that PIR sensors can detect a change in the infrared radiation levels. PIR sensors, together with PIR motion sensor cameras, measure infrared radiation levels to detect changes in the surroundings and can detect motion [18]. PIR sensors are very sensitive to any change in the incoming IR rays; even the smallest movements are registered. To increase reliability, we combine analog signals from multiple sensors in the system.

Based on the working principle of the PIR sensor presented [25] in the previous section, the analog sensor output depends on the following parameters: 1. difference in the overlapping area (a) of the subject's image with the two sensing elements, 2. distance of the subject from the PIR sensor (d), 3.time spent by the subject in the FoV of the PIR sensor (t), and 4.central angle of the sector the subject is traversing (Θ).

The camera surveillance is made for home surveillance [33], and the standard speed of internet speed for a house is 15 Mbps. The bandwidth of the internet connection is limited to several values. For this experiment, the internet bandwidths are limited by 15.3 Mbps, 12.6 Mbps, 10.11 Mbps, 6.89 Mbps, and 2.34 Mbps to see the frame per second performed by the system and determine the proper bandwidth for the best system performance, Research [37] suggested that 5G LTE-Ainitially provides and optimizes the flexibility and high data rates for the H2H communication including the classical mobile services.

The study [29] suggests that the threshold value distinguishes between bright and dark rooms. If the

opposition is higher than the resistance limit, it determines that one area is black. This study shows that the ideal image captured as a reference image. After that, the system will continuously capture images and compare them with the ideal image. If the ideal image and the picture taken have variations, there is motion detection.

Raspberry Pi is considered a very effective computing module for use in the use of IoT technology. Raspberry Pi is a low-cost credit card size computer [17] that plugs into a computer monitor or TV and uses a standard keyboard and mouse. Most importantly, it is open-source hardware with programmable computing language like Python and scratch under the Linux platform. The study [15] chose Raspberry Pi 2 as a computing module. Raspberry Pi is having the role of video compression. Webcam is having 1080p high definition video/image output [31]. [35] compile a table of differences between raspberries and other cards

Table.1 The difference bentween the Raspberry and Other cards

Card	*CPU*	*Architecture*	*RTOS economic supported*
Raspberry PI	Broadcom 700 MHz Broadcom 900 MHz	Cortex-A7/IDE	Linux (Raspbian, Debian GNU/Linux, Fedora, et Arch Linux ARM), RISC OS, FreeBSD,
Arduino/Atmel	ATmega32/32x, ATmega25 60	ATmega, ARM Cortex-M3/Arduino IDE	FreeRTOS, ChibiOS/RT
BeagleBoard and BeagleBone/TI	OMAP3/A M335x	ARM Cortex-A8/IAR Embedded Workbenchnull	Linux, Android, Ubuntu
Cerebot/microchip	dsPIC33f, PIC32MX	dsPIC, PIC32 (MIPS)/MPLAB IDE	FreeRTOS
ChipKit/micro chip	PIC32MX	PIC32 (MIPS)/MPLAB	FreeRTOS
Discovery/STMicroelectr onics	STM32	ARM Cortex/IAR Embedded	FreeRTOS, ChibiOS/RT
Freedom /Freescale	Kinetis K20 and KLxx	ARM Cortex-M0+/M4	MQX, MQX Lite

In this research [19] Pi raspberries are connected to the ZigBee module so that they form a transitive link with the sensor network. The processing unit is also connected via the ZigBee module to the display system. Raspberry Pi can be plugged into a TV, computer monitor, and it uses a standard keyboard and mouse [10]. To enroll and detect faces using a camera connected to the ARM Cortex of Raspberry Pi board. To recognize the correct face, it must match at least ten times with an existing flag. When face images are captured and trained, several positive and negative images are created. Capture.png, positive.png, negative.png, and mean.png files are created in the first instance after obtaining the confidence value [12].

Image processing using the Adaptive Motion Detection Method can be implemented and run smoothly by Raspberry Pi. With the help of a webcam, Raspberry Pi can capture images of movements that occur in the camera's viewing distance and then process the captured images of the movements that occur and send the detected motion to its users [4]. Research [5] uses Raspberry Pi with Python instruction language to communicate with AWS and IoT google logging web service by protocol OAuth.

A motion detector is a device that detects moving objects, particularly people. The security system captures information and transmits it via a WiFi to a static IP, which is viewed using a web browser from any smart device. Raspberry pi controls a video camera for surveillance. It streams live video and records the motion detected parts in the cloud and/ or in the windows shared folder for future playback. The cameras automatically initiate recording when motion is sensed, and the Raspberry pi device stores it in a secured folder [8].

To transmit data from the local sensor to the management database, it needs appropriate network technology. The study [28] found a fact of the results of trials where the system that sends the appropriate alarm message via SMS if a vehicle was stolen, or the GPS or GSM module did not function properly. The best design was proposed. The VAT system is integrated with the ThingSpeak and server Android application.

Vehicle anti-theft systems that are controlled remotely via GSM networks are highly recommended if cost-effectiveness, resource management, and owner's life are top priorities. Given this, it reduces losses for vehicle owners and allows the recovery of vehicles stolen easily by security agents or operators [24]. Project [24] the GPS module is used to track the currents vehicle location and sent it to the owner telephone via the GSM module. SIM900A module is a wireless technology device that renders support for a remote network service [22].

Dominant research recommends cloud-based data management, as summarized in the following study: in the study [9] described, Saving cloud-based data innate reliability, scalability, and cost-effectiveness, as they are scale horizontally, runs on cheap commodity hardware at distributed configuration. The cloud server applies YOLO object detection and records the objects [20]. Research [14] explains that Sensor Observation Service (SOS) is a Web service specifications determined by the Open Geospatial Consortium (OGC) Web Sensor Enablement (SWE) group for standardizing the way sensors and sensor data found and accessed on the Web.

Using the AWS IoT Device management console, it is easier to organize securely, monitor, and remotely manage IoT devices [16]. AWS has broad and deep IoT services, from the edge to the cloud. AWS IoT is the only cloud vendor to bring together data management and rich analytics in easy to use services designed for noisy IoT data [2]. AWS IoT is an IoT platform that is designed to enable meaningful connections between people and things. The features of IoT is real-time data collection, data analysis, data processing of the position information, data visualization, message transmission, etc. using a connected SNS, via an open-source API to support a various platforms Amazon Web Services of Internet of thing is permits secured [23]. AWS service called RDS (Relational Database System), which is hosted on a virtual instance in the cloud [30]. This remote storage makes it readily accessible to other applications that can give excellent deductions from the data.

Previous studies conducted the accuracy of the sensor height system, and the classification of object width in the object detection system with the PIR sensor is entirely

accurate to use. Research related to managing and sending data using the video streaming method and Motion camera produces two different methods. Video streaming emphasizes the real-time object detection process so that it can be processed earlier with human observation, but requires connectivity with a large enough bandwidth. While motion cameras require less bandwidth, but they need more time to identify objects accurately. In this case, study the use of motion cameras is appropriate because the location of many communication towers is in rural areas where GSM data connections still use 3G technology. In processing data objects, the server approach on-premises and cloud server has its advantages and is precisely implement according to the cases that will be resolve. In this case, it is more efficient to use the Cloud server; the growth of very aggressive communication tower construction can be support by cloud servers that have advantages in scalability.

In this article, we would like to introduce a method of utilizing appropriate technology to prevent cases of vandalism in communication towers. To detect human presence in communication tower areas as objects of vandalism, we use PIR Sensor, which is quite accurate, documenting objects using image systems because it is more efficient than large segments. Data, the computing module uses Raspberry Pi to process local data and control the camera device as a device to retrieve image data and a GSM transmission device for sending data. For managing our data, we use a more effective and scalable cloud service. Combining some of these technologies is expected to be able to prevent vandalism at an efficient cost.

3 PURPOSED METHODS

Based on the support of the theoretical foundation obtained from theoretical exploration, which uses as a conceptual reference of the research variable, a framework of thought can arrange as follows:

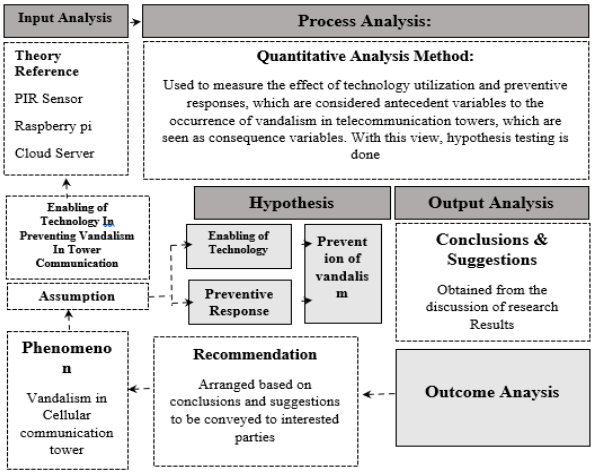

Fig. 3 Framework

The framework of thought illustrated in Figure 3 can explain as follows:

- Input analysis components include the phenomenon of suboptimal prevention of vandalism in cellular communication towers in Indonesia. Assumptions about the phenomenon, the title of the research that was born from the assumptions, and theories that become the reference for the preparation of operational concepts of research variables, namely the PIR Sensor Theory, Theory Raspberry Pi, and Cloud Server Theory.
- From such input analysis, a Process Analysis is carried out using the Quantitative Analysis Method. Quantitative analysis methods are used to measure the effect of technology utilization and preventive response, which seen as an antecedent variable (which precedes, causes) on the prevention of vandalism in cellular communication towers, which seen as a consequence variable in the framework of testing Hypotheses.
- Outputs Analysis These data analysis methods are the main Conclusions and Suggestions.
- Outcomes Analysis is a recommendation based on the main points of conclusions and suggestions obtained from the discussion of research results.
- With such a framework, it is assumed that there is a positive (unidirectional) effect of technology utilization and preventive response to vandalism in the communication tower, both partially and jointly.

The system design in this study consists of three stages: the planning stage, the literature review stage, and the deployment stage. The illustration in Figure 3.2 illustrates the order in designing this system, starting from the planning stage to be able to identify problems by conducting field studies following the data and facts expressed in the background Sub-chapter to formulate a problem. Then proceed to the literature review stage by collecting data and enabling technology models that have been applied in previous research studies, so getting the best. A suitable solution to implement preventing vandalism in the communication tower—studying the concepts and parameters that accompany the intended technology. The use of PIR sensors as object detectors that are considered to be able to validate human objects as subjects of vandalism, computational modules such as Arduino or Raspberry Pi. Raspberry Pi considers being more effectively use for transmitting an image or video data that will likely use in the subject validation and authorization process, data transmission with the GSM module, and cloud server. The next step is deployment.

The initial stage of this research is planning, which contains ideas or ideas that form the background of the study, as provided in section 1.1—namely contributing to the field of telecommunications by creating a theft prevention system for telecommunications equipment in telecommunications towers by utilizing existing technology. The literature review stage includes collecting data and enabling technology models that have been applied in previous research studies so that they get the best solution and are suitable to be

implemented in the case of preventing vandalism in the communication tower.

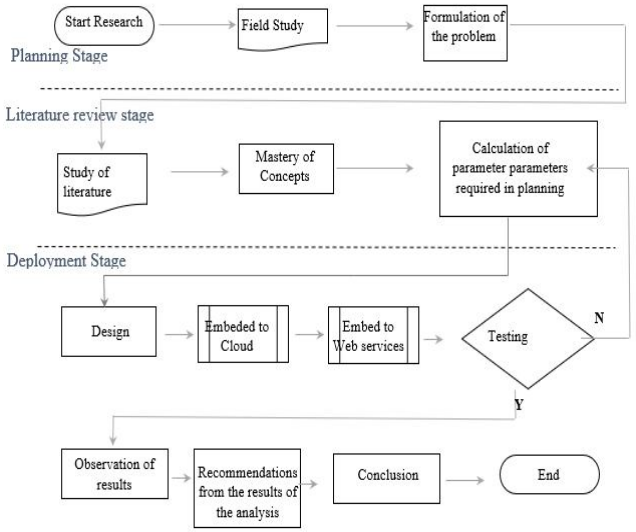

Fig. 4 System Design Process

Study the concepts and parameters that accompany the use of the technology in question. The final stage to be carried out is deployment, which starts from the design then is integrated into the cloud.

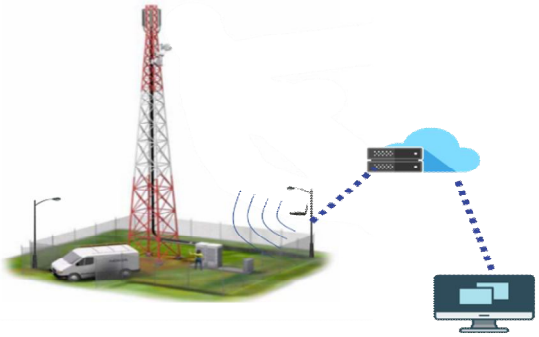

Fig. 5 Illustration of Communication System Topology

In this study, the authors recommend using Amazon Web Services (AWS) on the IoT feature embedded into the cloud server and desktop application. Then do the testing phase where a prototype device design to test the design so that a communication topology is forme, as illustrated in Figure 4. The results were observed and ended with the conclusions and recommendations of the research results.

Figure 5 divides two large blocks, namely the side fields that describe the position of the process in the communication tower or the field while monitoring the site position in the virtual process. In the field, the side block consists of a PIR sensor. As a sensor object that triggers the camera Trigger to take an image that is sent via GSM transmission to the server, all communication processes are managed in Raspberry Pi. In contrast, the Monitoring Side block is a virtual process through the Cloud Server and the monitoring and authentication decisions made by humans.

In Figure 5 divides two large blocks, namely the side fields that describe the position of the process in the communication tower or the field while monitoring the site position in the virtual process. In the field, side block consists of a PIR sensor, as a sensor object that triggers the camera Trigger to take an image which sent via GSM transmission to the server, all communication processes are managed in Raspberry Pi.

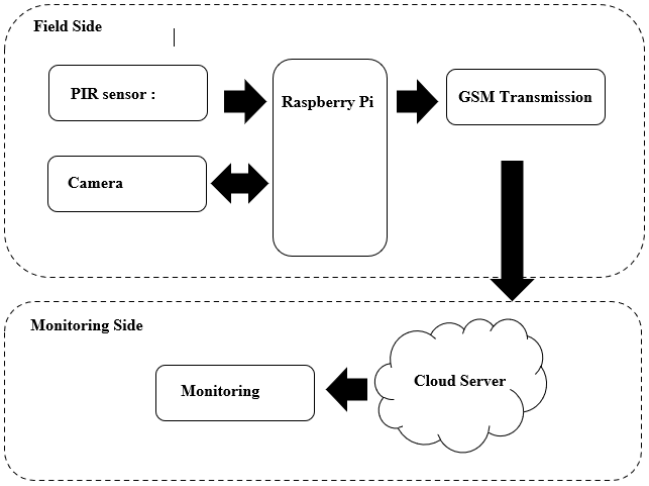

Fig. 6 Block diagram design

In contrast, the Monitoring Side block is a virtual process through the Cloud Server and the process of monitoring and authentication decisions made by humans.

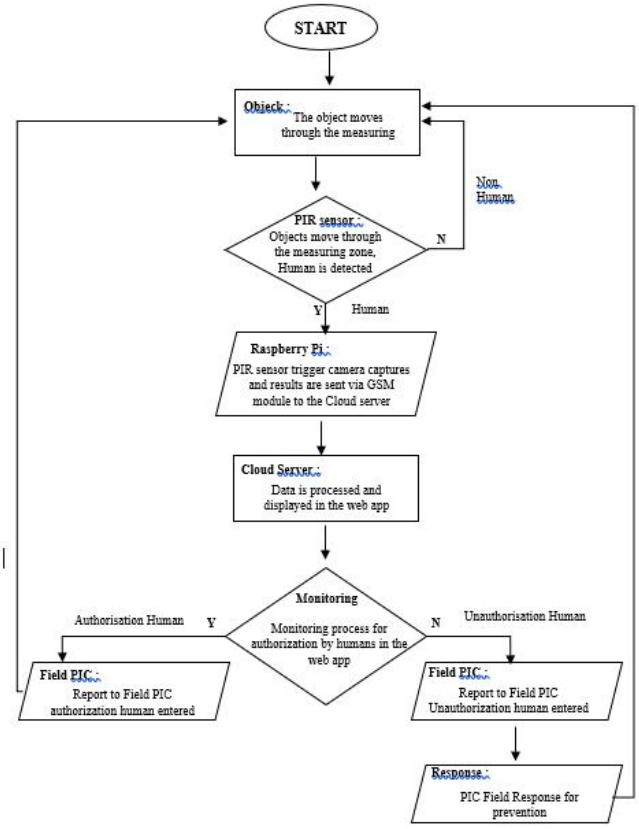

Fig. 7 Design flow chart

In this design, the process flow can be illustrated in Figure 7 with the explanation as follows:

- Objects - detected, in this case, moving objects, are in the PIR sensor coverage area
- PIR Sensor - Sensors detect moving objects which will only respond to human objects based on body temperature characteristics. If detected by humans, the information is forwarded to the Raspberry Pi to trigger the camera to take photos.
- Raspberry Pi - The process of controlling PIR sensors, cameras, and GSM transmission
- Cloud server - The process of storing and managing information and databases
- Monitoring - Displays information that has undergone the Computing process on the cloud server. It provides information for PIC monitoring to decide on the authorization of objects to access the communication tower area. In this case, the PIC ensures that humans detected by the PIR sensor permit access to previous site areas, such as engineers who carry out routine maintenance of communication devices.
- Field PIC - The party responsible for maintaining and maintaining the communication tower area equipment, in this case, site guards or tower technicians.
- Response - Actions carried out by the PIC to prevent vandalism

4 RESULT & DISCUSSION

Prototyping Hardware

As shown in Fig. 8 and 9, the prototype was built as an experimental tool in the use of technology to overcome the issue of vandalism in the communication Tower. The prototype uses the following devices and equipment:

1. PIR sensor
2. Camera
3. Circuit board
4. Raspberry Pi 3+
5. GSM modem

Which are then assembled according to the picture below

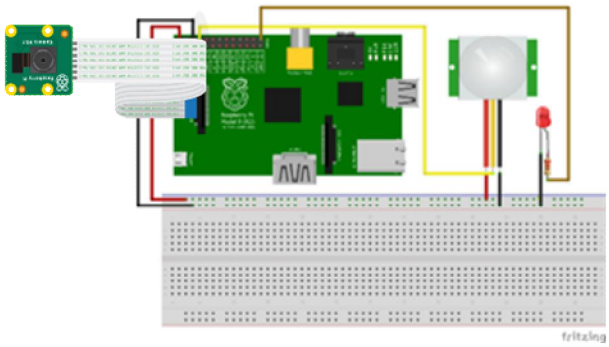

Fig. 8 Circuit diagram

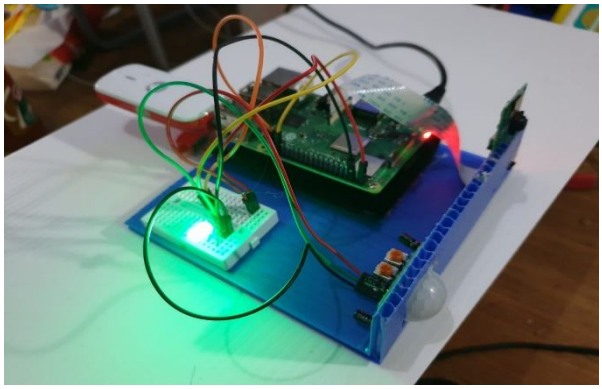

Fig. 9 Prototype

Coding

```
import RPi.GPIO as IO
import time, datetime
import telepot
import picamera
from telepot.loop import MessageLoop

IO.setwarnings(False)
IO.setmode(IO.BCM)

IO.setup(21,IO.OUT) #GPIO 2 -> Red LED as output
IO.setup(3,IO.OUT) #GPIO 3 -> Green LED as output
IO.setup(14,IO.IN) #GPIO 14 -> IR sensor as input

def action(msg):
   chat_id = msg['chat']['id']
   command = msg['text']
   global message

   if 'start' in command:
      telegram_bot.sendMessage(chat_id,'Welcome to the
bot')
      while True:
         if(IO.input(14)==False): #object is far away
            IO.output(21,1) #Red led ON
            telegram_bot.sendMessage(chat_id,'Motion
Detected')
            telegram_bot.sendMessage(chat_id,'Capturing
photo...')
            print("Capturing photo...")
            cameraEnable = True
            camera = picamera.PiCamera()
            camera.capture('./photo.jpg')
            camera.close()
            telegram_bot.sendMessage(chat_id,'Sending
photo...')
            print("Sending photo to ")
            telegram_bot.sendPhoto(chat_id, photo =
open('./photo.jpg'))
         else:
            IO.output(21,False) #Red led ON
            time.sleep(1)
```

```
telegram_bot =
telepot.Bot('1172155324:AAE61KAP2Phg_crrFuVm8XY_G
hDqnSQK0Jc')
print(telegram_bot.getMe())

MessageLoop(telegram_bot, action).run_as_thread()
print('up and Running')

cameraEnable = False
while 1:
   time.sleep(10)
```

Experimental

Experimental stages:

1. run the coding file (Tele.py) on the raspberry pi terminal
   Python tele.py
2. Give the command message "Start" on Telegram to start the standby process

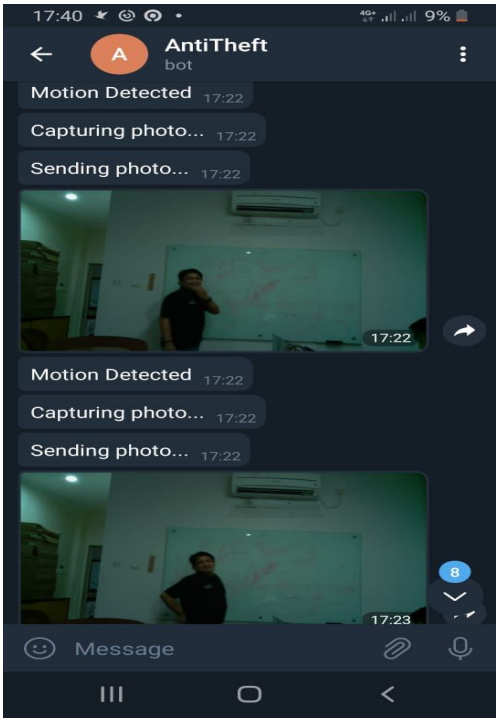

Fig. 10 the results of data reception in the telegram application

In Figure 10, we can see the object detection process results, taking photos of objects to send photos to Telegram Bot to validate object authorization. The process from the above stages is very fast under 1 second; this proves that the use of IoT technology and preventing vandalism in communication towers is more effective than traditional methods, as seen in the following Table 2.

Table 2. Comparison of response time

Table of comparison of response times to objects of perpetrators of vandalism between traditional methods using iot			
	Object Detection	Verification Object	Response
Traditional Methode	00:00':00"	02:00':00"	02:00':00"
With IoT	00:00':00"	00:00':01"	00:00':01"

5 CONCLUSION & FUTURE WORKS

From the experimental results using the IoT device, the resulting capture of a moving object is captured correctly with the camera and sent quickly to a Telegram app. The time required from capturing the object movement to receiving the object photo is very fast so that the response to those who want to commit vandalism can be made more quickly.

This technology can be developed for more functional and effective results, namely by using face detection with the open-source computer vision library, so that the object verification process can be faster and more accurate. In the development of science, the technology from this research is not novel, but it has a very big influence on the business efficiency of GSM service providers.

6 ACKNOWLEDGEMENT

This research was support by the company PT XL Axiata Tbk. We are grateful to our colleagues from many departments in the company PT Mitra Karsa Utama, who provided insight and expertise that greatly helped this research and my colleagues at Bina Nusantara (class 1922).

REFERENCES

1. Akhil, T., Aruna, B., Praveen, S., & Bharathi, K.(March 2019). Sensors Enabled For Anti-Thefting System.
2. Amazon Web Services (AWS).. Amazon Web Services (AWS). https://aws.amazon.com/. Accessed 25 january 2020
3. An, X., Lu, P., Wei, N., & Hong, G. (2018).. Design of power cable grounding wire anti-theft monitoring system. E&ES, 108(5), 052121.
4. Antonius, A., Triyanto, D., & Ruslianto, I. (2015).. Penerapan Pengolahan Citra Dengan Metode Adaptive Motion Detection Algorithm Pada Sistem Kamera Keamanan Dengan Push Notification Ke Smartphone Android. Coding Jurnal Komputer dan Aplikasi, 3(2).
5. Basha, S. N., Jilani, S. A. K., & Arun, M. S. (2016). An intelligent door system using Raspberry Pi and Amazon

web services IOT. International Journal of Engineering Trends and Technology (IJETT), 33(2), 84-89.

6. Brijet, Z., Kumar, B. S., & Bharathi, N. (2017).. Vehicle Anti-Theft System Using Fingerprint Recognition Technique. Open Academic Journal of Advanced Science and Technology, 1(1), 36-41.
7. Chen, N., Di, L., Yu, G., & Min, M. (2009).. A flexible geospatial sensor observation service for diverse sensor data based on Web service. ISPRS Journal of Photogrammetry and Remote Sensing, 64(2), 234-242.
8. Dasgupta, Rhythm. (2017).. Motion Activated Wireless Surveillance Security Camera Using Raspberry Pi. 10.13140/RG.2.2.31134.02886.
9. Dey, S., Chakraborty, A., Naskar, S., & Misra, P. (2012, October).. Smart city surveillance: Leveraging benefits of cloud data stores. In 37th Annual IEEE Conference on Local Computer Networks-Workshops (pp. 868-876). IEEE.
10. Fezari, M., Dahoud, A.A., (2019).. Internet of Things (IOT) Using Raspberry Pi Retrieved from https://www.researchgate.net/publication/330513589_Internet_of_Things_IOT_Using_Raspberry_Pi. (Terakhir dikunjungi 20 September 2019).
11. Gu, Y., Kim, M., Cui, Y., Lee, H., Choi, O., Pyeon, M., & Kim, J. (2013, June).. Design and implementation of UPnP-based surveillance camera system for home security. In 2013 International Conference on Information Science and Applications (ICISA) (pp. 1-4). IEEE.
12. Gupta, I., Patil, V., Kadam, C., & Dumbre, S. (2016, December).. Face detection and recognition using Raspberry Pi. In 2016 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE) (pp. 83-86). IEEE.
13. Hamid, S. B. A., Rosli, A. D., Ismail, W., & Rosli, A. Z. (2012, November).. Design and implementation of RFID-based anti-theft system. In 2012 IEEE International Conference on Control System, Computing and Engineering (pp. 452-457). IEEE.
14. Henson, C. A., Pschorr, J. K., Sheth, A. P., & Thirunarayan, K. (2009, May).. SemSOS: Semantic sensor observation service. In 2009 International Symposium on Collaborative Technologies and Systems (pp. 44-53). IEEE.
15. Hossain, N., Kabir, M. T., Rahman, T. R., Hossen, M. S., & Salauddin, F. (2015, November).. A real-time surveillance mini-rover based on OpenCV-Python-JAVA using Raspberry Pi 2. In 2015 IEEE International Conference on Control System, Computing and Engineering (ICCSCE) (pp. 476-481). IEEE.
16. Jukić, O., Špeh, I., & Heđi, I. (2018, May).. Cloud-based services for the Internet of Things. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 0372-0377). IEEE.
17. Kulkarni, B. P., Joshi, A. V., Jadhav, V. V., & Dhamange, A. T. (2017).. IOT Based Home Automation Using Raspberry Pi. International Journal of Innovative Studies in Sciences and Engineering Technology, 3(4), 13-16.
18. Kumar, K. K., Natraj, H., & Jacob, T. P. (2017, April).. Motion activated security camera using Raspberry Pi. In 2017 International Conference on Communication and Signal Processing (ICCSP) (pp. 1598-1601). IEEE.
19. Lakshmisudha, K., Hegde, S., Kale, N., & Iyer, S. (2016).. Smart Precision Based Agriculture Using Sensors. International Journal of Computer Applications, 146(11), 36-38.
20. Layek, M. A., Uddin, A. S., Hossain, M. D., Thu, N. T., Yu, S., Yong, C. H., ... & Huh, E. N. (2018).. Cloud-based Smart Surveillance System using Raspberry Pi and YOLO. 한국정보과학회 학술발표논문집, 510-512.
21. Liu, Z., Wang, M., Qi, S., & Yang, C. (2019).. Study on the Anti-Theft Technology of Museum Cultural Relics Based on Internet of Things. IEEE Access, 7, 111387-111395.
22. Lukman, A. J. A. O., EMMANUEL, A., Chinonso, N., Mutiu, A., James, A., & Jonathan, K. (2018).. An Anti-Theft Oil Pipeline Vandalism Detection: Embedded System Development. International Journal of Engineering Science and Application, 2(2), 55-64.
23. Manjula, T., Sreenivasulu, U., & Hussain, S. J. (2016).. A dynamic Raspberry Pi sense HAT multimodality alerting system by using AWS IoT. Indian Journal of Science and Technology, 9, 0974-5645.
24. Mohammed Shafeeq, K. K., & Maqbool Thoufeeq, T. (2018).. Android Board Based Intelligent Car Anti-Theft System Through Face Recognition Using GSM and GPS. Journal of Applied Information Science, 6(2), 01-05.
25. Mukhopadhyay, B., Srirangarajan, S., & Kar, S. (2018).. Modeling the analog response of passive infrared sensor. Sensors and Actuators A: Physical, 279, 65-74.
26. Narayana, S., Prasad, R. V., Rao, V. S., Prabhakar, T. V., Kowshik, S. S., & Iyer, M. S. (2015, April).. PIR sensors: Characterization and novel localization technique. In Proceedings of the 14th international conference on information processing in sensor networks (pp. 142-153). ACM.
27. Oladimeji, T. T., Oshevire, P. O., Omitola, O. O., & Adedokun, O. E. (2013).. Design and Implementation of Remotely Controlled Vehicle Anti-Theft System via GSM Network. Wireless Sensor Network, 2013.
28. Paing, S. N., Oo, M. Z., Othman, M., & Funabiki, N. (2019).. A Personal Use Vehicle Anti-Theft Tracking System Using IoT Platform. International Journal of Computer & Software Engineering, 2019.
29. Patil, N., Ambatkar, S., & Kakde, S. (2017, April).. IoT based smart surveillance security system using raspberry Pi. In 2017 International Conference on Communication and Signal Processing (ICCSP) (pp. 0344-0348). IEEE.

30. Patil, R. M., Srinivas, R., Rohith, Y., Vinay, N. R., & Pratiba, D. (2017, December).. IoT Enabled Video Surveillance System Using Raspberry Pi. In 2017 2nd International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS) (pp. 1-7). IEEE.
31. Shete, R., & Sabale, M. (2015).. VIDEO SURVEILLANCE USING RASPBERRY PI ARCHITECTURE. In International Conference On Computing, Communication, Electrical Electronics, Devices And Signal Processing (Cceeds), March
32. Sun, J., Zhang, Z., & Sun, X. (2016).. The intelligent crude oil anti-theft system based on IoT under different scenarios. Procedia Computer Science, 96, 1581-1588.
33. Surya, E., & Ningsih, Y. K. (2019).. Smart Monitoring System Using Raspberry Pi and Smartphone. ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika, 7(1), 72. https://ejurnal.itenas.ac.id/index.php/elkomika/article/view/2317 (terakhir dikunjungi 21 september 2019)
34. Chen, Y. C., Chen, R. S., Sun, H. M., & Wu, S. F. (2019). Using RFID technology to develop an intelligent equipment lock management system. *International Journal of Computational Science and Engineering*, *20*(2), 157-165.
35. Kortas, N., & Arbia, A. B. (2019). Development and evaluation of the cloudlet technology within the Raspberry Pi. *International Journal of Computational Science and Engineering*, *19*(4), 464-473.
36. S. Kevin Andrews, V.Jeyabalaraja, M.S.Josephine (2019). Vehicle Information System using R-Pi and Internet of Things. *International Journal of Advanced Trends in Computer Science and Engineering. ISSN 2278-3091*
37. Radhia Khdhir , Aymen Belghith. (2019). 5G LTE-A Cognitive Multiclass Scheduling Scheme for InternetofThings Internet of Things. *International Journal of Advanced Trends in Computer Science and Engineering. ISSN 2278-3091*