IoT-Based Multi-Sensor Security System for Intrusion Detection in BTS Towers

Fanny Julia Rezki[a], Firdaus[b], Vera Veronika[c], Shinta Marviola[d]*

[a]*D4 Telecommunication Engineering Study Program, Department of Electrical Engineering, Padang State Polytechnic Jl.Kampus, Limau Manis, Kec.Pauh, Padang City, West Sumatra 25164, Indonesia*

Corresponding author: [a]fannyjuliarezki@gmail.com

***Abstract*— The Tower Base Transceiver Station (BTS) is an essential telecommunications infrastructure susceptible to theft and vandalism, particularly in isolated areas with limited oversight, potentially resulting in financial losses and service disruptions. The primary aim of this study is to devise and execute a dependable and cost-effective security system to mitigate such hazards. The research presents a cohesive security solution utilizing the Internet of Things (IoT), amalgamating many essential technologies for thorough surveillance. The designed system comprises Passive Infrared (PIR) sensors for detecting human activity at tower access points, SW-420 vibration sensors for identifying physical shocks or attempted breaches in perimeter fences, and intelligent CCTV for direct visual verification. The complete system is governed by an ESP8266 microcontroller that analyzes sensor data and transmits real-time notifications to operators using the Telegram application. The development technique encompasses hardware integration, microcontroller programming via the Arduino IDE, and configuration of the IoT platform. Field testing was performed using intrusion simulation scenarios to assess sensor precision and notification delay. The findings demonstrated that the system functioned dependably, with the vibrating sensor detecting interference at a distance of 8 meters and the PIR sensor accurately identifying movement within a vertical range of 4 meters. The use of this solution enhances BTS tower monitoring, facilitates expedited threat response, and markedly bolsters asset protection. The research functions as a scalable framework for safeguarding additional vital infrastructures in remote areas.**

Keywords—IoT, smart CCTV, PIR sensor, vibration sensor, ESP8266, Telegram

Manuscript received 06 Nov. 2025; revised 26 Apr. 2026; accepted 26 Apr. 2026. Date of publication 12 Mei. 2026.

I. INTRODUCTION

Base Transceiver Station (BTS) towers are critical components of telecommunications infrastructure, enabling wireless communication between operator networks and user devices. In response to the increasing demand for internet connectivity, telecommunications providers are systematically upgrading their networks by installing additional BTS towers in various locations. Nonetheless, these towers are often located in remote areas with limited supervision, making them prime targets for asset theft [1].

The pilferage of infrastructure at BTS sites remains a significant threat to the telecommunications industry. This illicit activity incurs substantial financial losses for operators and immediately disrupts communication services for the public. A clear case of security vulnerabilities occurred at the PNN304 site in the Mandeh region, which saw two theft events involving telecommunications equipment within a designated window. The confiscated equipment included Remote Radio Units (RRUs), critical components that amplify signals and connect antennas to the central processing system. The lack of this equipment caused signal disturbance and impeded communication access in the surrounding area. The persistent incidence of thefts at the same location indicates that existing security vulnerabilities remain inadequately addressed.

Multiple pertinent studies have investigated the progression of security devices. Fausan [2] developed a tower security system employing an ESP32-CAM that sends photographic alerts via Telegram upon object detection by the PIR sensor. A pertinent study by Kusuma and Sipayung [3] developed a prototype for detecting battery theft in towers, employing NodeMCU ESP8266, PIR sensors, and GPS modules that relay Google Maps URLs over Telegram upon motion detection. Furthermore, research conducted by Pangaribuan et al. [4] devised an anti-theft alarm system for stationary automobiles,

employing a PIR sensor to detect body heat and a vibration sensor (SW-420) to sense external vibrations, with processing managed by an Arduino Uno R3.

This study introduces a novel approach that integrates the SW-420 vibration sensor, PIR sensor, and ESP8266 microcontroller. The system has been enhanced with an intelligent CCTV camera that facilitates direct monitoring via a website and may generate real-time alert notifications. Upon identifying a disturbance, alerts are transmitted to Telegram, creating a dual-layered alert system. This project is to provide an efficient IoT-based security solution to improve BTS monitoring, prevent equipment theft, and provide prompt, real-time alert notifications.

II. LITERATURE REVIEW

A. Internet of Things (IoT)

The Internet of Things (IoT) facilitates the connectivity and data sharing of physical things through the Internet, eliminating the need for direct human-computer contact. In the realm of security systems, the Internet of Things (IoT) is crucial as it facilitates remote surveillance and automated reactions to possible attacks. Satria [6] asserts that the implementation of IoT in security systems enhances operational efficiency and diminishes the expenses associated with manual surveillance. Consequently, the Internet of Things serves as the fundamental foundation for the advancement of sensor-driven security systems that are accessible in real time.

B. PIR (Passive Infrared) Sensor

A PIR sensor is an electrical device that identifies variations in infrared radiation released by nearby objects, especially the human body, which possesses a greater temperature than its surroundings. The HC-SR501 sensor utilized in this studyThis study employed a PIR sensor to monitor human movement near the BTS tower steps for the prompt and precise identification of suspicious conduct.y possesses a detection range of up to 7 meters with an angle of 120° and functions at a voltage of 4.5V to 12V [8]. This sensor operates based on its response to variations in heat radiation detected by the Fresnel lens.

C. SW-420 Vibration Sensor

The SW-420 vibration sensor is a digital device that identifies physical shocks or vibrations and transforms them into electrical impulses. This sensor operates as a typically closed switch that activates or deactivates based on the vibration intensity. The sensitivity may be modified by an inbuilt potentiometer, and it functions on a 3.3V–5V DC power source [9]. This study employed the SW-420 sensor to identify vibrations on the BTS tower fence resulting from incursion attempts or unauthorized physical action, so functioning as the primary layer of security detection.

D. NodeMCU ESP8266

The NodeMCU ESP8266 is a microcontroller-based IoT platform featuring an embedded Wi-Fi module that provides wireless communication in accordance with the 802.11 b/g/n standard. This apparatus is equipped with an 80 MHz CPU and 4 MB of flash memory, facilitating efficient sensor data processing [10]. The minimal power consumption and user-friendly programming capabilities render NodeMCU an optimal selection for small to medium-scale IoT systems. In this study, NodeMCU functions as a control unit that oversees data from PIR and vibration sensors and transmits notifications using the Telegram platform.

E. Telegram Bot API

Telegram has a Bot API that enables developers to construct automated messaging services and combine them with other IoT devices. This feature provides robust security via end-to-end encryption and eliminates the need for a dedicated server, enhancing cost-efficiency [15]. Riry et al. [15] shown that the Telegram Bot API is effective for transmitting real-time notifications in microcontroller-based control systems. This study utilized Telegram to transmit automatic notifications to operators upon the detection of disturbances in the BTS tower vicinity by the sensors.

F. Research Related to BTS Security Systems

A considerable amount of study has been undertaken about the implementation of IoT in the security of BTS towers. Sharma et al. [16] devised an IoT-based smart security system for rural regions, incorporating many sensors to identify intrusion activities. Al-Khasawneh [17] performed a comprehensive analysis of the security of Low Power and Lossy Networks (LLNs) inside Internet of Things (IoT) contexts, a significant difficulty in remote monitoring systems. Kumar and Obaidat [18] suggested an IoT-based framework for the security of critical infrastructure, encompassing telecommunication towers.

Tripathy et al. [19] presented iSENSE, an IoT-driven intelligent framework designed for the monitoring and safeguarding of telecommunication towers through the utilization of diverse sensors and machine learning techniques. Saha et al. [20] created a GSM-based remote monitoring system for base transceiver stations (BTS) that transmits notifications via SMS upon detection of suspicious activities. These studies show that the integration of IoT and sensor technology significantly enhances the security of telecommunications infrastructure.

This paper offers an IoT-based BTS security system utilizing a multi-sensor method that integrates PIR sensors, SW-420 vibration sensors, and intelligent closed-circuit television (CCTV). This method is anticipated to deliver a more efficient, quick, and cost-effective option for safeguarding the BTS infrastructure in remote regions.

III. RESEARCH METHODOLOGY

This research was executed in multiple phases, encompassing hardware design, software development, and system integration. The primary aim was to develop an automated security system for cellular towers by integrating many essential electronic components and employing IoT technologies to deliver real-time alerts.

A. System Design

This design emphasizes the system's cost-effectiveness and dependability. The NodeMCU ESP8266 was selected over alternative microcontrollers like the Raspberry Pi due to its inbuilt WiFi module and reduced power consumption, making it suitable for a straightforward yet efficient notification system. Telegram was selected as the notification platform because to its robust Bot API, facilitating seamless integration and offering rapid, secure, and complimentary real-time communications without requiring a dedicated server [15].

The system architecture is depicted in the block diagram presented in Figure 1. The NodeMCU ESP8266 functioned as the primary control unit, managing data from all linked sensors. The input components comprise a PIR sensor for movement detection and a vibration sensor for detecting physical disruptions to the fence. Upon detecting a potential threat, the NodeMCU transmits an alert across the Internet to a prepared Telegram bot. A sophisticated CCTV functions concurrently to deliver visual verification, with the complete system underpinned by a reliable power source to guarantee its uninterrupted operation.

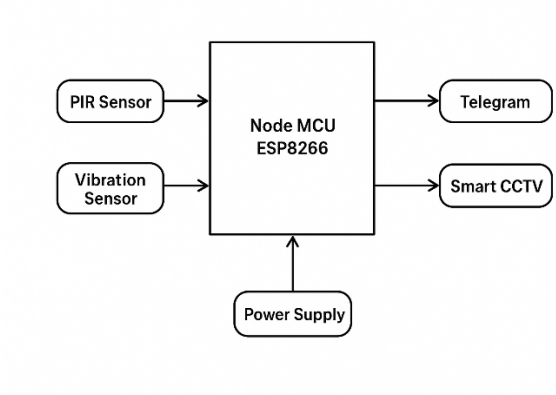

Fig. 1 Block Diagram of the Security System

B. Hardware Components

Table I delineates the principal technical specifications of the primary hardware components utilized in this study. This pick was predicated on a balance of performance, cost, and integration simplicity.

TABLE I
Technical Specifications of Hardware Components

Component	Key Specification	Purpose in System
NodeMCU ESP8266	80 MHz CPU, 4MB Flash, Wi-Fi	Central processing and IoT gateway
PIR Sensor (HC-SR501)	7-meter range, 120° angle	Motion detection on the tower ladder
Vibration Sensor (SW-420)	Digital Output (High/Low)	Intrusion detection on the fence
Smart CCTV Bardi	355° Pan, 60° Tilt, 2.4GHz Wi-Fi	Live visual verification

1) NodeMCU ESP8266: An open-source Internet of Things platform that functions as the system's central processing unit. This module analyzes sensor inputs and regulates the notification systems. The module was specifically intended for Internet connectivity, featuring 4 MB of flash memory and supporting wireless technologies 802.11 b/g/n [10].
2) PIR Sensor (HC-SR501): a passive infrared sensor utilized for motion detection by reacting to infrared radiation released by the human body. The sensor possesses a detection range of roughly 7 meters at an angle of 120° and functions with an input voltage between 4.5 V and 12 V, delivering a 3.3 V TTL output signal [8].
3) Vibration sensor (SW-420): a digital device that identifies vibrations and transforms them into electrical impulses. This sensor operates as a typically closed switch that activates and deactivates in reaction to vibration. The sensitivity can be modified using an integrated potentiometer. The Sensor functions with a DC power supply ranging from 3.3 V to 5 V.
4) Bardi smart CCTV: an outdoor IP camera that transmits video and audio directly to a smartphone. The camera features pan-tilt-zoom (PTZ) functionality, enabling a horizontal rotation of 355° and a vertical rotation of 60° for enhanced surveillance coverage. The camera possesses an IP65 classification, indicating its resistance to water splashes, and it connects to the network over a 2.4 GHz WiFi connection [12].
5) 5) Supporting components: A breadboard facilitates the construction of prototype circuits without the need for soldering. Jumper cables (male-to-male and male-to-female) facilitated the connection between the sensor and the NodeMCU. Power adapters transform large AC voltages into steady low DC voltages necessary for electronic components [13].

C. Software Design and Implementation

The system logic was created via flowcharts, as illustrated in Figure 2. The procedure commences with the initialization of the ESP8266, which connects to the Wi-Fi network and activates the sensor pins. The system subsequently engaged in a continuous monitoring loop, acquiring data from the PIR and vibration sensors. In the absence of disruption, the system persists in standby mode. Upon activation of any sensor, the NodeMCU promptly transmits a notification message to the user over a Telegram bot. This bot was developed via BotFather on Telegram, which supplies an API key for the integration of ESP8266 with Telegram services [15].

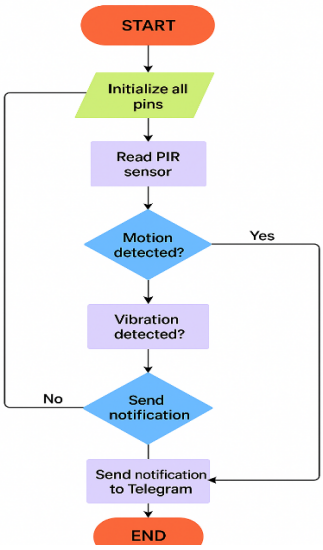

Fig. 2 System Flowchart

Microcontroller programming is executed utilizing the Arduino IDE with the C++ programming language. The software code incorporates a WiFi library for network connectivity, a UniversalTelegramBot library for interfacing with the Telegram server, and digital pin configurations for monitoring sensor status. The communication protocol employs HTTPS over port 443 with TLSv1.2 encryption to guarantee data security [14].

D. Research Location and Time

This research was performed at the PNN304 BTS site situated in the Mandeh region of West Sumatra. The site was selected due to its history of theft and its distant position with minimal supervision. System testing was conducted over three months to assess system performance under diverse environmental conditions.

E. Testing Procedures

Testing was performed in several stages.

1. Connectivity Testing: Assessing the NodeMCU's capability to connect to the Wi-Fi network and Telegram server using network traffic analysis utilizing Wireshark [14].
2. 2. PIR sensor evaluation: The vertical and horizontal detection ranges were assessed by positioning the sensor at a height of 4 meters and evaluating the response of test participants at varying distances.
3. 3. Vibration sensor evaluation: The detection efficacy was assessed by introducing disturbances to the fence at distances of 1, 3, 5, 8, and 11 meters from the sensor installation locations.
4. 4. System integration testing: Simulated intrusion scenarios were executed to assess the entire system response, including the notice delivery time.

IV. RESULTS AND DISCUSSION

This section delineates the outcomes derived from the field testing of the BTS tower security system. The assessment concentrated on system connection and the efficacy of PIR and vibration sensors in identifying potential intrusions.

A. System Connectivity and Notifications

Preliminary testing was performed to confirm that the NodeMCU ESP8266 module could effectively connect to the Wi-Fi network and interact with the Telegram server. The module acquired the local IP address 192.168.1.5 and was verified as active on the network using ICMP echo requests (ping) from other devices.

Network traffic analysis conducted with Wireshark [14] revealed that the ESP8266 established a secure connection to the Telegram cloud server (103.10.124.92, 103.10.124.84) through port 443 utilizing the TLSv1.2 protocol. This verifies that all data, including notification messages, is encrypted during transmission. Upon sensor activation, the system effectively transmitted real-time notifications to the designated Telegram bot, thereby confirming the end-to-end communication functionality.

B. PIR Sensor Performance

The PIR sensor was positioned on the primary entrance stairway of the tower at an elevation of roughly 4 meters, oriented downward to especially oversee this entry point. This test aimed to ascertain the sensor's effective vertical and horizontal detection ranges. The findings are encapsulated in Table II.

TABLE II
Performance Test Of The Pir Sensor

PIR Sensor Position	Detected by Sensor	Notification Delivery Time
1 meter (directly below sensor)	Yes	2 seconds
2 meters (directly below sensor)	Yes	2 seconds
3 meters (directly below sensor)	Yes	2 seconds
4 meters (directly below sensor)	Yes	4 seconds
4m with 0.5m offset to the right	Yes	15 seconds
4m with 0.5m offset to the left	Yes	17 seconds
4m with 1m offset to the right	No	-
4m with 1m offset to the left	No	-

The test findings indicated that the PIR sensor functioned optimum when sensing human presence directly beneath it at a vertical distance of 1–3 m. At a distance of 4 m, the sensor's reaction exhibited reduced speed and inconsistency. Detection was successfully achieved horizontally at a distance of 0.5 m to either the left or right of the central point, however with a

considerable delay in notification transmission. The sensor was unable to detect any movement at a lateral distance of 1 meter. This signifies a limited detecting angle, ideally suited for its purpose of overseeing direct access to stairs while reducing false alerts from the vicinity.

C. Vibration Sensor Performance

The SW-420 vibration sensor was evaluated by affixing one sensor to each of the three accessible sides of an 11.2-meter-long wire fence. The test sought to evaluate the sensor's capability to detect vibrations generated by an individual interacting with the fence at different distances. The findings are displayed in Table III..

TABLE III
Performance Test of The Vibration Sensor (Sw-420)

Vibration Test Distance	Detected by Sensor	Notification Delivery Time
1 meter	Yes	1 second
3 meters	Yes	1 second
5 meters	Yes	3 seconds
8 meters	Yes	10 seconds
11 meters	No	-

The vibration sensor is highly efficient, precisely identifying vibrations up to 8 meters from the installation site with a rapid response time. At the maximum evaluated distance of 11 m, the sensor's reaction exhibited considerable latency, requiring up to 11 seconds to activate a notification. The performance constraint arises from the flexible and lightweight characteristics of the wire fence, which attenuates the transmission of vibrations over extended distances.

D. Discussion

1) PIR Sensor Performance Analysis

Discrepancies in PIR sensor efficacy underscore the significance of appropriate sensor positioning. The substantial rise in notification delay when the target was positioned outside the center (from 4 seconds to over 15 seconds) was likely attributable to the target's location outside the periphery of the Fresnel lens detection zone of the sensor. This leads to a diminished infrared signal reaching the pyroelectric sensor, hence necessitating additional time to activate an alert. Hidayat and Sapudin [7] elucidated that the Fresnel lens properties of the HC-SR501 PIR sensor exhibit an optimal detection zone centrally, diminishing towards the periphery.

The effective vertical detection range of 4 m aligns with the sensor's technical specifications, which indicate a maximum range of 7 m [8]. The disparity can be attributed to the sensor's vertical orientation and the restricted detection angle when positioned lower. This arrangement is beneficial for stair monitoring applications since it minimizes the likelihood of false alarms from surrounding activities near the tower.

2) Vibration Sensor Performance Analysis

The failure of vibration sensors at a distance of 11 m can be ascribed to the physical characteristics of chain-link fencing, which presumably attenuates vibration waves prior to their arrival at the sensor module. Pangaribuan et al. [4] discovered in their study that the SW-420 sensor exhibits diminished efficacy at distances above 8 m when mounted on flexible constructions.

The rapid response time (1 second) at a distance of 1-3 meters demonstrates the sensor's high sensitivity to direct vibrations. The rise in response time at a distance of 8 m (10 s) signifies a substantial reduction in vibration amplitude. To enhance coverage, it may be advisable to incorporate additional sensors at reduced intervals or utilize a fence constructed from a morehard material that can effectively transmit vibrations.

3) Comparison with Previous Research

In comparison to prior research, our system provides a more extensive security solution. The system created by Fausan [2] solely concentrates on gathering visual evidence post-incident, whereas our system incorporates an early detection mechanism via vibration sensors, hence offering timely alerts.

In contrast to the GPS-based system suggested by Kusuma and Sipayung [3], which monitors assets post-theft, our methodology is focused on preventing intrusions. Our system's multi-sensor integration offers a resilient and anticipatory security framework.

Sharma et al. [16] and Tripathy et al. [19] employed a multi-sensor methodology for the security of critical infrastructure in their studies. Nonetheless, their systems incorporate more expensive components, including Raspberry Pi and high-resolution cameras. Our technology provides a cost-effective alternative that retains efficacy for conditions in Indonesia, particularly for BTS installations in rural areas.

4) Obstacles to Implementation

Field testing revealed numerous challenges inherent to the deployment environment. The positioning of the towers in mountainous and rural areas resulted in erroneous alerts triggered by wildlife, including poultry and avian species, as well as by vigorous gusts that caused the fences to vibrate. These occurrences highlighted the fundamental deficiencies of the system. To address this issue, intelligent CCTV cameras were installed as an additional security measure. These cameras offer instantaneous visual verification for each alert produced by the sensors, assisting users in distinguishing between genuine dangers and false alarms.

Currently, sensor notifications are efficiently integrated into a cohesive alert system through Telegram, whereas CCTV notifications operate via a separate proprietary program. This requires users to switch between two separate applications to achieve a comprehensive understanding of the security state. Kumar and Obaidat [18] suggested that integrating all monitoring components into a single platform will improve user experience and response efficacy.

5) Constraints and Suggestions for Enhancement

Multiple restrictions were identified during on-site testing. The system's dependence on a singular WiFi connection, coupled with misleading warnings induced by environmental factors, presents a potential single point of failure. Network disruptions or intentional WiFi interference may disable the notification system. Subsequent iterations may explore the integration of supplementary communication channels, such as a GSM module for transmitting SMS notifications as a contingency, akin to the methodology employed by Saha et al. [20].

Power consumption remains unoptimized, and for deployment in areas without a dependable power supply, solar-powered solutions with battery backups should be considered. Al-khasawneh [17] emphasizes the importance of energy efficiency in IoT systems for remote infrastructure. Implementing signal filtering algorithms or alternative sensor reading techniques can reduce false alarms, hence improving the system's overall reliability.

V. CONCLUSION

This research successfully designed and implemented an IoT-enabled security system for BTS towers using ESP8266 microcontrollers, PIR sensors, SW-420 vibration sensors, and advanced CCTV technology. The system functions effectively as a dual-layer security solution. The hardware components are strategically placed, allowing the vibration sensor to accurately detect disturbances up to ±8 meters along the fence, while the PIR sensor provides dependable motion detection up to 4 meters with a focused vertical angle.

The system facilitates rapid remote monitoring via two methods: it dispatches automatic text notifications through a Telegram bot upon sensor activation, and it offers real-time video access through a dedicated smart CCTV application. This ensures that operators can respond promptly to imminent threats.

To facilitate future growth, the system might be significantly improved by integrating all monitoring components—sensor alerts and real-time CCTV feeds—into a unified Android application. This will streamline the monitoring process and enhance the user experience. Furthermore, utilizing signal filtering or other sensor reading techniques can help reduce false alarms caused by environmental factors such as strong winds or wildlife, hence improving the system's overall reliability.

It is recommended to improve system resilience in remote regions by integrating redundant communication modules such as GSM for SMS backup and optimizing energy consumption using renewable resources. This work provides pragmatic contributions via economical and efficient security solutions for telecommunications infrastructure in Indonesia, particularly for BTS stations located in areas with limited surveillance accessibility.

REFERENCES

[1] J. Prihatin, R. T. Shita, dan S. Waluyo, "Title of Paper," dalam *Proc. 2nd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, Jakarta, Indonesia, 2023, hlm. xx-xx.

[2] A. M. Fausan, "Perancangan dan Implementasi Sistem Keamanan Pada Tower Komunikasi Berbasis ESP32 Cam," Tesis Magister, Jurusan Teknik Elektro, Telkom University, Bandung, Indonesia, 2021.

[3] K. Kusuma dan E. M. Sipayung, "Perancangan Prototype Pendeteksi Lokasi Pencurian Baterai Tower Berbasis Internet of Things," dipresentasikan pada Konferensi Ilmiah Mahasiswa Tingkat Nasional, 2022.

[4] J. H. C. Pangaribuan, I. Gunawan, H. S. T., Sumarno, dan I. O. Kirana, "Perancangan Alarm Anti Maling Pada Kendaraan Bermotor Dalam Posisi Parkir Menggunakan Sensor PIR (Passive Infrared Receiver) Dan Sensor Getar Berbasis Arduino Uno R3," *Jurnal Teknik*, vol. x, no. x, hlm. xx-xx, Jan. 2021.

[5] G. Hergika, "Perancangan Internet of Things (IoT) Sebagai Kontrol Infrastuktur dan Peralatan Toll Pada PT. Astra Infratoll Road," *Jurnal XYZ*, vol. 8, no. 2, hlm. xx-xx, 2021.

[6] I. H. Satria, *Buku Ajar Internet of Things*. Medan, Indonesia: Insight Mediatama, 2021.

[7] M. R. Hidayat dan B. S. Sapudin, "Perancangan Sistem Keamanan Rumah Berbasis IoT dengan NodeMCU ESP8266 Menggunakan Sensor PIR HC SR501 dan Sensor Smoke Detector," *Jurnal Listrik, Instrumentasi, dan Elektronika Terapan (JuLIET)*, vol. 7, no. 2, hlm. xx-xx, 2018.

[8] Components101, "HC-SR501 PIR Sensor," *components101.com*. Diakses: 22 Jan. 2025. [Daring]. Tersedia: https://components101.com/sensors/hc-sr501-pir-sensor

[9] R. H. Setiawan, "Rancang Bangun Sistem Penilaian Ujian Praktik SIM C," Tesis Magister, Univ. Mercu Buana, Yogyakarta, Indonesia, 2019.

[10] T. Sulistyorini, N. Sofi, dan E. Sova, "Pemanfaatan Nodemcu ESP8266 Berbasis Android (Blynk) Sebagai Alat Mematikan dan Menghidupkan Lampu," *JUIT*, vol. 1, no. 3, hlm. xx-xx, 2022.

[11] A. Rizky dan U. Latifa, "Smart Parking Distance System Menggunakan Aplikasi Android," *Jurnal Ilmiah Wahana Pendidikan*, vol. 2024, no. 3, hlm. 63-72, Feb. 2024, DOI: 10.5281/zenodo.10633802.

[12] PT. BARDI Solusi Otomasi, "IP Camera Outdoor PTZ (Lite Version)," *bardi.co.id*. Diakses: 06 Feb. 2025. [Daring]. Tersedia: https://bardi.co.id/product/ip-camera-outdoor-ptz-lite-version/

[13] A. Sander dan D. Pujianto, "Membangun Perangkat Bilik Masker Otomatis Untuk Pencegahan COVID-19," *Jurnal Abdimas Mandiri*, vol. x, no. x, hlm. xx-xx, 2022.

[14] I. P. A. E. Pratama dan P. A. Dharmesta, "Implementasi Wireshark Dalam Melakukan Pemantauan Protocol Jaringan (Studi Kasus: Intranet Jurusan Teknologi Informasi Universitas Udayana)," *Jurnal Ilmiah Teknologi Informasi dan Komputer*, vol. 03, hlm. 94-99, 2019.

[15] A. D. Riry, L. Wattimury, dan J. D. C. Sihasale, "Perancangan IoT Sistem Kendali Pada Peralatan Elektronik Rumah Tangga Dengan Menggunakan Telegram Bot Berbasis Mikrokontroler," *JURNAL ISOMETRI*, vol. 2, no. 2, hlm. xx-xx, 2023.

[16] P. K. Sharma, A. Singh, dan R. G. Mishra, "An IoT-Based Smart Security and Monitoring System for Remote Areas," dalam *Proc. 2018 4th Int. Conf. on Computing Communication and Automation (ICCCA)*, Greater Noida, India, 2018, hlm. 1-5, DOI: 10.1109/CCAA.2018.8628437.

[17] M. A. A. Al-khasawneh, "A Survey on the Security of Low Power and Lossy Networks (LLNs) in the Internet of Things (IoT)," *J. Netw. Comput. Appl.*, vol. 169, Nov. 2020, Art. no. 102781, DOI: 10.1016/j.jnca.2020.102781.

[18] S. Kumar, dan M. S. Obaidat, "An IoT-based framework for securing and monitoring of smart critical infrastructures," *Ad Hoc Networks*, vol. 86, hlm. 15-22, Apr. 2019, DOI: 10.1016/j.adhoc.2018.11.002.

[19] A. A. Tripathy, S. P. Mohanty, S. Kougianos, E. Kougianos, dan D. P. Agrawal, "iSENSE: An IoT-based Intelligent Framework for Monitoring and Securing Telecommunication Towers," dalam *Proc. 2019 IEEE Int. Conf. on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2019, hlm. 1-6, DOI: 10.1109/ICCE.2019.8662057.

[20] H. N. Saha, A. Roy, dan R. Karlose, "A GSM-Based Remote Surveillance System for BTS," dalam *Proc. 2013 Annual IEEE India Conf. (INDICON)*, Mumbai, India, 2013, hlm. 1-5, DOI: 10.1109/INDICON.2013.6726055.