Jurnal Teknik dan Keselamatan Transportasi

ISSN: 2622-0105 (print) | 2716-1196 (online)
http://jurnal.poltekbangmakassar.ac.id/

Design of a Security Cameras for Smart Rooms Based on Internet of Things (IoT) as an Automation Learning Media at Makassar Aviation Polytechnic

Muhammad Fikri[1], Ahmad Rossydi[2], Ahmad Risal[3]
Politeknik Penerbangan Makassar[1,2], Universitas Negeri Makassar[3]

Article info

Received: 24-07-2024
Final Revision: 04-12-2024
Accepted: 20-11-2024
Available online: 27-12-2024

Keywords:

Building Automation
Automation System, security, ESP32 CAM, PIR sensor, Trainer,

ABSTRACT

This research is essential as it directly addresses the growing need for enhanced security and modern educational tools in learning environments, particularly in technical and aviation fields. By integrating IoT-based security cameras into smart rooms, the study ensures a safer campus environment and provides students and instructors with immediate and practical benefits. They gain hands-on experience in cutting-edge automation technologies, which not only enhances their learning but also prepares them for the real-world application of these skills. At Makassar Aviation Polytechnic, where precision, safety, and innovation are core values, this research bridges theoretical learning and practical application, equipping students with the skills necessary for the rapidly evolving fields of aviation technology and IoT implementation. The research questions focus on how to design, do feasibility tests, and integrate usefully as a learning medium for practical tools in the form of an Automation System Trainer at the Makassar Aviation Polytechnic. This research aims to develop IoT-based security cameras for smart rooms, enhancing real-time surveillance and providing an innovative learning tool. It seeks to improve safety and operational efficiency at Makassar Aviation Polytechnic while promoting student proficiency in IoT and automation, aligning with the technological demands of the aviation industry. The method used in this research is R&D (research and development) with a waterfall type of research, which involves conducting research design, designing tools, providing tool components, and carrying out testing after the entire system is built. The tool was then tested for suitability using an instrument in the form of a questionnaire given to 2 experts in their fields at the integration and testing stage to ensure the tool's usefulness. The results of this research show that the system works according to the desired design and can be integrated with other devices so that an automation system is formed in the building, where when the PIR sensor detects movement, the ESP32 CAM will take an image and send a message to the Telegram website.

Recommended Citation:

APA Style

INTRODUCTION

The urgency of this research lies in the growing need for secure, technology-integrated educational environments in response to advancements in IoT and automation. At Makassar Aviation Polytechnic, where precision and safety are critical, integrating IoT-based security cameras into bright rooms addresses immediate concerns for enhanced campus safety while simultaneously serving as an innovative learning medium. This dual-purpose approach ensures students gain hands-on experience with cutting-edge technologies, equipping them with essential skills to thrive in the rapidly evolving aviation industry. Delaying this integration risks falling behind in educational quality and campus security standards.

There has been significant interest in integrating IoT with security systems in recent years, especially for innovative environments such as smart homes and classrooms. A study by Jain et al. (2021) explored how IoT-based security systems can enhance safety and surveillance in bright spaces, using real-time monitoring and cloud-based data processing to provide an efficient security solution. The authors discussed the design of smart surveillance cameras with IoT capabilities, which can be integrated with motion detection, alert systems, and video analysis features. The study concluded that such IoT-based systems are ideal for educational environments, where security is crucial for students and staff.

In another study, Ahmad et al. (2020) examined the use of IoT devices in smart classrooms, focusing on automation and security functionalities. The researchers proposed a system that integrated IoT-based cameras, environmental sensors, and automated access control systems within the learning space. The study found that security cameras, when connected to a cloud platform, allowed real-time monitoring and video analytics, offering both automation of learning environments and enhanced security. They also noted that such systems could improve the management of educational facilities, providing students and instructors with a more controlled and secure learning space.

Kumar and Patel (2019) proposed a model for integrating IoT-based surveillance cameras into smart classrooms for automated learning environments. The model utilized real-time video streaming from cameras integrated with IoT sensors, offering security features such as motion detection, unauthorized entry alerts, and intelligent analytics. Their work highlighted the role of these technologies in reducing the need for manual surveillance and making educational institutions safer and more efficient. The research also discussed the potential challenges in implementing IoT surveillance in terms of data privacy and network security.

A study by Singh and Gupta (2022) focused on designing and implementing innovative security systems using IoT for educational institutions, particularly in technical institutes. Their research proposed a security camera system that provided video surveillance and integrated various sensors (e.g., temperature, motion, and gas) for monitoring different environmental factors. The system was designed to be user-friendly, with a mobile app interface allowing easy monitoring and control. The researchers found that IoT-based security cameras in an innovative room environment offered enhanced security, ease of use, and the ability to manage the system remotely.

An automation system uses technology to perform tasks automatically without significant human intervention. The main goal of an automation system is to increase efficiency, productivity, and consistency in a particular process or operation. Common characteristics of automation systems include using hardware and software to control and manage specific tasks. Technological progress embodies an era of change that brings increasingly modern human progress (Yurita, I., Ramadhan, M. K., & Candra, M., 2023). Advances in automation technology make important contributions in various fields, including safety and security. Using sensors, intelligent software, and system integration are key foundations for developing solutions that can handle emergencies effectively. Security automation systems refer to the use of automated technology to monitor, control, and respond to situations related to security aspects.

Security should not be ignored; therefore, a security system must be created with good security and can be monitored in every process (Koroy, A. M. S. & Muhammad; A. H., 2020). If the system is intended to protect people, property, or the environment from potential hazards or dangerous events. A sound security system still requires supervision by a security guard. To ensure security, security guards must stand in front of the screen and monitor the objects captured by the camera. Therefore, security becomes very important. The room security system is essential. The security system in certain rooms, such as locked rooms, is also fundamental, mainly if the room is used to store valuable items. Therefore, we need a system that can monitor or monitor the room in real-time and monitor the room from a narrow-angle. Please note that currently, at the Makassar Aviation Technology Institute, there is no learning media in the form of an automation system trainer to understand how automation system equipment works and build the system yourself.

A study by Wang et al. (2020) delves into the implementation of IoT-based innovative security systems in educational institutions, including surveillance cameras and automated monitoring tools. The researchers highlight how IoT can significantly improve security by providing continuous surveillance through connected devices, enabling instant alerts for unauthorized activities, and reducing human intervention. They focus on the security and data management challenges when integrating IoT devices into educational space.

In their 2021 research, Kumar and Yadav (2021) explored the integration of IoT devices for creating smart classrooms, with a specific focus on security cameras. Their paper discusses implementing real-time video surveillance systems, where cameras are interconnected with motion detection sensors and cloud-based platforms to manage data storage and real-time monitoring. The system can be used for educational automation and security, enabling educators and administrators to monitor activities remotely.

Zhang et al. (2022) investigated the role of security cameras within IoT frameworks for innovative learning environments. They proposed integrating IoT devices such as cameras, motion sensors, and door access controls to create a secure and efficient learning space. The system's ability to automate surveillance and control access based on IoT data is a crucial improvement in campus security and operational efficiency in educational settings.

In their 2020 study, Lee and Kim (2020) explored how IoT-based security cameras can be designed for smart buildings, including educational environments. The study presents an innovative security system architecture that uses connected cameras to enhance surveillance capabilities, reduce security risks, and ensure real-time monitoring. The authors emphasize the potential for IoT to transform educational spaces by providing automated responses to detected incidents.

Based on the explanation above, the writer makes a comparative summary below:

Study	Strengths	Weaknesses
Wang et al. (2020)	Comprehensive coverage, future trends, and data security focus	Lacks case studies, overemphasis on challenges
Kumar and Yadav (2021)	Real-time monitoring, integration of security, and automation	Narrow focus on classrooms, lack of scalability discussion
Zhang et al. (2022)	Holistic approach, detailed architecture, integration with environmental sensors	Limited evaluation, focus on learning environments only
Lee and Kim (2020)	Case study approach, the broader context of smart buildings	Limited scope of case study, technological limitations in the solution
Zhang and Wang (2021)	Cloud integration, data analytics, scalability	Dependence on the internet, lack of discussion on privacy concerns

Each of these studies brings valuable insights to the table, especially in the context of IoT-based security cameras for smart educational environments. However, there are notable differences in terms of scope, practical application, and future implications. Some papers provide a more comprehensive theoretical foundation, while others offer real-world case studies or focus on specific aspects like cloud integration or real-time data analytics.

METHOD

The type of research used in this research is research and development (R&D). Research and development methods are research methods used to produce a particular product and test the effectiveness of the product. In the research project Design of Security Cameras for Smart Rooms Based on the Internet of Things (IoT) as an Automation Learning Media at Makassar Aviation Polytechnic, the Waterfall model is used to guide the systematic and structured development of the IoT-enabled security camera system. The process begins with the requirements gathering and analysis phase, where the specific needs of the innovative room environment are identified. This includes determining the security features, such as real-time video monitoring, motion detection, and integration with IoT devices like smart thermostats or door locks. The system must also align with the educational goals of Makassar Aviation Polytechnic, ensuring that it functions both as a security system and an automated learning tool for students. Next, in the system design phase, the architecture for the security camera system is developed, which includes deciding on camera placement, defining IoT connectivity protocols, and designing the user interface for real-time monitoring. This phase also considers how the system will integrate with other smart room technologies to enable automation, such as triggering alarms or adjusting the environment based on detected motion. During the implementation phase, the cameras and IoT devices are physically installed, followed by software development that will connect these devices and allow centralized control and monitoring. This phase also includes creating user interfaces to interact with the system, ensuring the technology is accessible and practical for educational use.

Once the system is built, the integration and testing phase begins. This involves ensuring that all components—cameras, IoT sensors, and software—work seamlessly together, with extensive testing to confirm that the system functions as expected. Special attention is given to security aspects, ensuring that video data is transmitted securely and that users have appropriate access permissions. The deployment phase follows, where the system is launched in the smart rooms, and real-world testing occurs. This includes adjusting the system for practical issues and training students and faculty on using the system effectively as a learning tool.

Airman: Jurnal Teknik dan Keselamatan Transportasi
Volume 7 Issue 2 December 2024 | page 14-29
DOI: http//doi.org/10.46509/ajtk.v7i2.510

Finally, in the maintenance and updates phase, the system is regularly monitored for performance issues, and updates are released to improve functionality, fix bugs, or introduce new features. This waterfall approach ensures that the design and development process is orderly, with each step building on the previous one, resulting in a robust and effective security camera system supporting security and educational objectives at Makassar Aviation Polytechnic.

The waterfall model is currently a commonly used software development model. This model takes a systematic and sequential approach. The stages in this model start from the planning stage to the management stage (maintenance) and are carried out in stages. Developers need to know more about the system development process when using the waterfall model and also the characteristics of the waterfall model (Wahid, A. A., 2020). This is called a waterfall because each stage that is passed is waiting for the previous stage to complete and must occur one after another. This development model runs linearly from the initial stage of system development, or planning stage, to the final stage of system development or maintenance stage. The next stage is not implemented until the previous stage is completed, and you cannot go back or repeat the previous stage. Based on this analysis, we propose a new pragmatic framework for socio-technical systems engineering (STSE) that builds on the research of (largely independent) groups investigating job design, information systems, computer-supported cooperative work, and cognitive systems engineering (Sommerville, 2011). For the development model, it can be analogous to a waterfall, where each stage is carried out sequentially from top to bottom. There are five stages in the waterfall method; the first is a requirement, which explains the understanding of the needs needed in the design, which includes hardware and software in designing the device.

Requirement: At this stage, system developers must communicate to understand what software users expect and their limitations. Information can be obtained through interviews, discussions, or direct surveys. Information is analyzed to obtain the data needed by users. At this stage, developers create a system design to help determine hardware and system requirements and define the overall system architecture. Implementation: In this stage, the system is first developed in small programs called units, which are integrated in subsequent stages. Each unit is developed and tested for functionality, which is referred to as unit testing. Verification: At this stage, the system is verified and tested to see whether the system entirely or partially meets the system requirements. Testing can be categorized into unit testing (carried out on a specific module of code), system testing (to see how the system reacts when all the modules are integrated), and acceptance testing. (conducted with or on behalf of the customer to see if all customer needs are satisfied). Maintenance: This is the final stage of the waterfall method. The finished software is run and maintained. Maintenance includes correcting errors that were not found in previous steps.

On the results of this test, the author carried out the test using data analysis techniques using quantitative analysis using an instrument in the form of a questionnaire. Validation testing of the Trainer for Security Cameras on Building Automation Systems involves several steps to ensure that the data obtained is valid and reliable. Two experts in the field examined this questionnaire directly, and the validity of the tool's work will be assessed. The author tested with two experts in the field, namely Mr. Muhammad Agung Raharjo, S.Kom., M.A.P., and Mr. Heru Prasetyo, M.Kom. The following are the results of the following test

The formula used to calculate the percentage on the Likert scale is as follows

$$xi = \frac{\sum s}{smax} \times 100\%$$

Information :
smax = Maximum score
$\sum$s = Total score
xi = Feasibility value for each aspect

Based on the results of calculations using the formula above, the test results on the two validation test questionnaires using two experts in their fields, show that this device included in the very feasible category.

System Design

As for how this research tool works, it can be seen in the following picture:

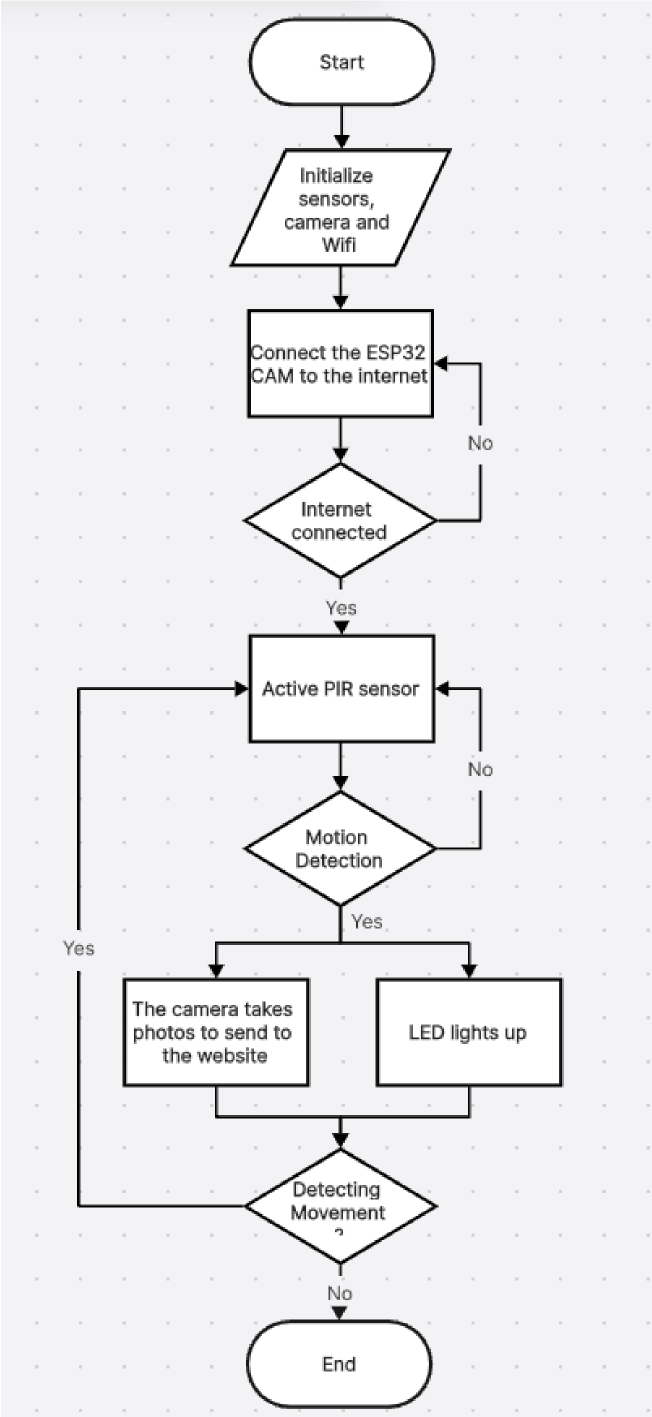

Figure 2 Tool Work Flowchart

In the flowchart image of how this tool works, the first thing is to initialize what inputs are used in this tool, where the inputs in the design of this tool are the PIR sensor, ESP32 CAM, and Wi-Fi. Then, the ESP32 CAM module will be connected to the internet; when the ESP32 CAM module is connected to the internet, the PIR sensor will be active, the PIR sensor will work to detect movement, then the output from the Arduino Uno will activate the buzzer and the ESP32 CAM module will take a photo of the detected image and will send data or such information to the WEBSITE. Next, the PIR sensor will continue to detect movement; if not, the PIR sensor will continue to work to detect movement, and the buzzer will turn off.

Device Components

The components used to make tools can be hardware and software.

A. Hardware

Following is a list of components used in the hardware:

a) The Arduino UNO functions as a circuit controller and a place to embed programs that will process input and output data to activate the buzzer.
b) Buzzer as a means to make sound.
c) ESP32 CAM platform that can monitor in real time by using a camera, and is able to connect to a WiFi module.
d) The PIR sensor functions as a human movement detection sensor.
e) Laptop/Pc to create the program you want to use.

B. Software

Following is a list of components used in the software:

a) WEBSITE as a platform for monitoring.
b) Bot Telegram for receive image information
c) The Arduino IDE is useful for editing, creating, uploading boards, and coding certain programs.

Device Design

The first step in designing a room security system based on telegram notifications is to create a block diagram which is a basic description of this system, so that the entire block diagram of the circuit will produce a tool that can work in accordance with the research objectives. The block diagram of the system can be seen in the image below

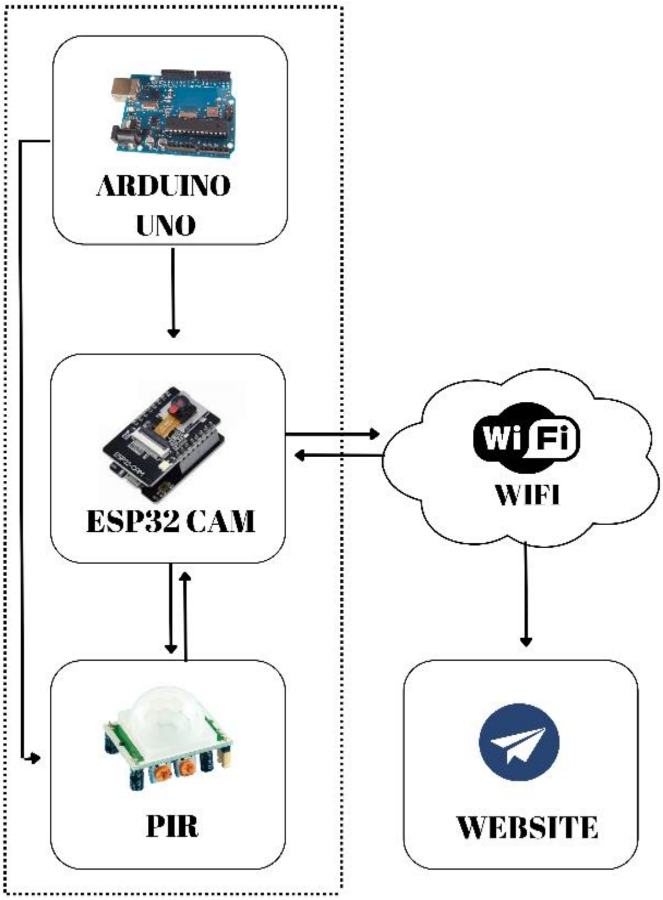

Figure 3 Device Design

Airman: Jurnal Teknik dan Keselamatan Transportasi
Volume 7 Issue 2 December 2024 | page 14-29
DOI: http//doi.org/10.46509/ajtk.v7i2.510

The explanation of each block is as follows:

1. Wifi/hostpot to connect the ESP32 CAM to the internet without using cables. The wifi/hostpot device can be an access point modem or smartphone hotspot or laptop.
2. ESP32 CAM as the central controller. The ESP32 CAM is integrated with a camera and WiFi so it can connect to the internet. The ESP32 CAM is also connected to a PIR sensor.
3. PIR sensor to detect human presence/movement. Then trigger the ESP32 CAM to capture the image.
4. Arduino Uno is useful as a power supply for the ESP32 CAM and PIR sensor.
5. WEBSITE as a Log Book facility, where information will be entered and can be monitored.

The next step is to design a block diagram of all the equipment that will be integrated into the Trainer Building Automation System, below is the block diagram of the Trainer Building Automation System that has been created

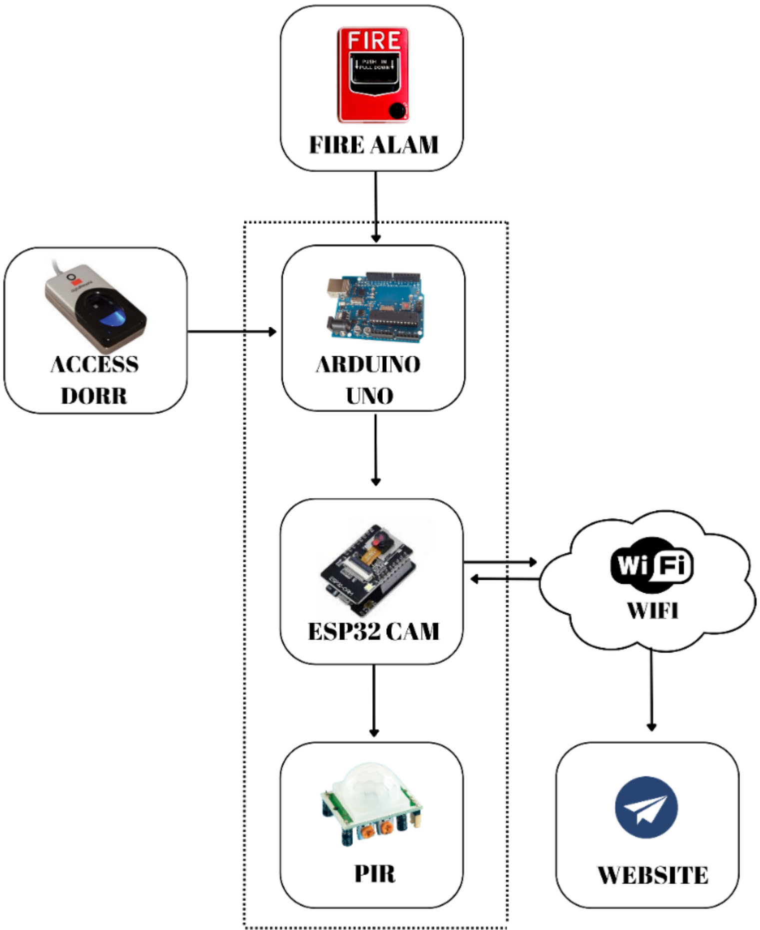

Figure 4 Blok Diagram BAS

In the block diagram above created by the author, the equipment is integrated with the access control and fire alarm systems, and these three devices are controlled by one brain - a microcontroller and monitored on the WEBSITE as a means of monitoring. The components on the dotted line are tool components made by the author, namely a Security CAM that uses an ESP32 CAM and also a PIR sensor. Components outside the dotted line are tools created by other researchers who are part of the same group of authors, namely Design of a Trainer Building Automation System Based on Internet of Things (IoT) with access control and fire alarm systems, and the block diagram above is a conversion tools created by other researchers become tools created by the author, and are integrated with each other. The website in the block diagram above is a website created by other researchers to monitor integrated tools so that all devices can be controlled by a central controller and monitored and supervised on one website.

Testing Techniques

At this stage, the researcher will test the tools on the design that has been created to test the feasibility of the Security Camera design for the Internet of Things Based Building Automation System Trainer at the Makassar Aviation Polytechnic using a quantitative approach in the form of a questionnaire as an assessment instrument. This questionnaire will be given to two experts who have relevant expertise and experience in their fields, with the aim of gathering their views and assessments regarding the feasibility of the tool that has been designed.

Data Analysis Technique

From the planning explained previously, the author will use data analysis techniques using quantitative analysis by giving questionnaires to two experts in their fields. classification of scores according to the Likert scale

Table 1. Product Feasibility Categories

Category	Score
Very Agree	5
Agree	4
Enough	3
Don't agree	2
Very Disagree	1

The formula used to calculate the percentage on the Likert scale is as follows

$$xi = \frac{\sum s}{smax} \times 100\%$$

Information :
smax = Maximum score
∑s = Total score
xi = Feasibility value for each aspect
Then to classify the results as worthy of passing the test or not, you can use the following categories:

Tabel 2 Product Eligibility Category

Eligibility Interval	Category
81%-100%	Very Worth It
61%-80%	Worthy
41%-60%	Not Worth It
21%-40%	Not feasible
0%-20%	Totally Not Worth It

RESULTS AND DISCUSSION

The author raises the title Security Camera Design for Internet of Things-based Building Automation System Trainers at the Makassar Aviation Polytechnic, in order to act as a learning trainer at the Makassar Aviation Polytechnic which can give students an overview and function of this tool which will later be found in the field. This research is useful for providing alternative solutions to users in order to increase efficiency and effectiveness in the student learning process at Makassar Aviation Polytechnic. Security cameras themselves function as surveillance and surveillance cameras that can monitor situations and capture human movements in confined spaces in real-time.

The following is a schematic image of the Security Camera circuit, which can be seen in the following image:

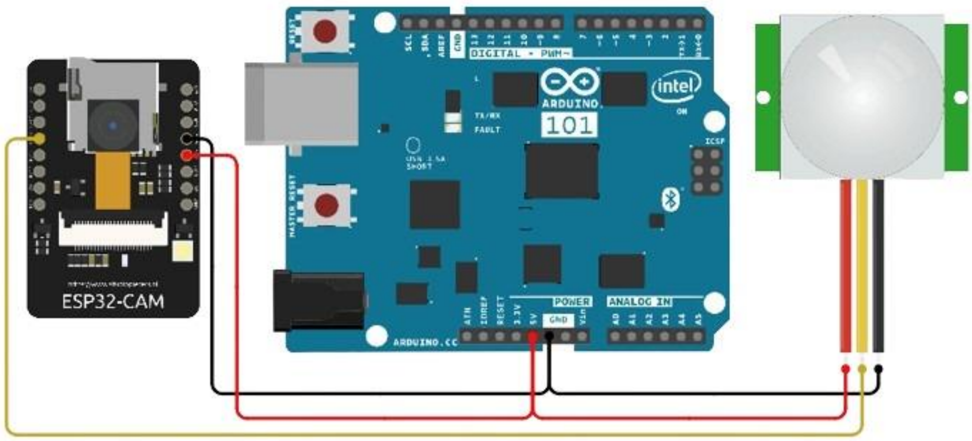

Figure 5 Equipment circuit schematic

Based on the picture above, you can see the ESP32 CAM as the processing center. The PIR sensor has 3 pins, namely Vcc, Dout and Gnd. The Arduino UNO is useful as a power supply for the ESP32 CAM and PIR sensor, the 5v pin and GND pin of the Arduino UNO are connected to the Vcc pin and GND pin of the ESP32 CAM and PIR sensor. On the ESP32-CAM module, IO pin 13 is often used as one of the digital input/output pins which can be configured for various functions, including communicating with external sensors such as PIR (Passive Infrared) sensors. If the IO pin 13 on the ESP32-CAM is connected to the output pin on the PIR sensor, then this pin functions as an input to receive signals from the PIR sensor.

The PIR sensor functions to detect motion, by capturing heat energy produced from the passive infrared rays of each object, which will trigger the ESP32 CAM to capture an image, which then sends a notification to a telegram bot that has been integrated with the WEBSITE that has been created by members of the writing group. , if someone is detected in the room, it will send a message and photo to the telegram bot with the information "THERE IS MOVEMENT!!!". The PIR sensor is used to sense movement and the control center uses an Esp32 CAM microcontroller. In the telegram bot that has been created, there are 3 optional features, namely /start to activate the program, /photo to take direct photos of the room, /flash to activate the lights on the camera.

The advantage of the ESP32 CAM microcontroller is that apart from the integrated WiFi module, Bluetooth, micro SD slot, there is an OV2640 camera with 2 MP quality. Meanwhile, the disadvantage of the ESP32 CAM is that if the operating voltage drops or is less than 5 volts, the quality of the image sent will not be good. For further details, based on the results of the research that has been carried out, the system is declared successful in running according to the desired design. For more details, see the image below:

Airman: Jurnal Teknik dan Keselamatan Transportasi
Volume 7 Issue 2 December 2024 | page 14-29
DOI: http//doi.org/10.46509/ajtk.v7i2.510

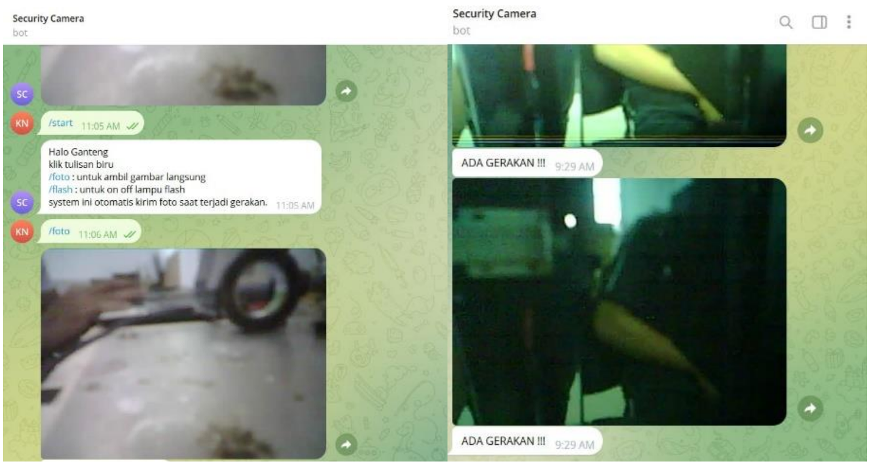

Figure 6 Telegram View

In designing the trainer for Security Cameras made by the author, this tool can work because there are several similarities to tools made by several other researchers, such as (Kurniawan, 2018) "Internet of Things: Home Security System Based on Raspberry Pi and Telegram Messenger". The system is able to work to detect, record and send the results to the user. (Khozainuz Zuhri and Ahmad Ihkwan, 2020) research "Designing a Telegram-Based Multiple Security System Using an ESP32-CAM Microcontroller". Using ESP32 CAM as a surveillance camera. (Ruhwan, 2020) "Movement Detection Using PIR Sensors for SMS-Based Room Security Systems." Uses a pir sensor to detect movement when leaving the room. (Emilia Hesti, 2012) "Design of a moving monitoring camera system with a pir sensor (transmitter)". By using a moving camera monitoring system with a PIR sensor. And also (Ardiansyah, 2023) "Design a telegram-based home security system using ESP 32 CAM". The researcher created a telegram-based home security system using Esp32-Cam, the results of which will be accessed on the Android mini PC screen by controlling the IP camera and detecting movement using a web-based IP camera, the results of which are capable of providing notifications on the Android application (Telegram) and alarm alerts.

However, the difference between the author's tools is that the tools created by the author are integrated with tools created by other researchers in one group, namely the Building Automation System. That is what differentiates this research from previous research.

Table 3 Indicators of Success

No.	Parameter	Success Indicators	Test result
1.	ESP32 CAM	Capture images with and in real time.	The test results were declared successful because it was able to capture images automatically when there was movement.
2.	Sensor PIR	Can detect movement well.	The test results were declared successful because it could detect when there was movement passing in front of the PIR sensor.
3.	Arduino UNO	Arduino UNO as the power supply for the tool.	The test results were declared successful because the Arduino UNO was able to provide power to the ESP32 CAM and PIR sensor.

The weaknesses of the Trainer for Security Cameras are:

The ESP32-CAM has several disadvantages. Here are some of them, Camera Quality: The image quality of the built-in camera (OV2640) is not comparable to high-quality cameras. Images may lack sharpness and detail, especially in low-light conditions. Wi-Fi Stability: The Wi-Fi connection on the ESP32-CAM can be unstable, especially if the Wi-Fi signal is not strong or there is a lot of interference. Limited Connectivity: The ESP32-CAM does not have many GPIO pins available as many of the pins are used by the camera module, which may limit the ability to add additional hardware.

The weakness of the PIR (Passive Infrared) sensor is that it is a sensor used to detect movement based on changes in infrared radiation around it. Although very useful in a variety of applications, PIR sensors have several disadvantages, Limited Motion Detection: The PIR sensor can only detect movement that occurs within its range and viewing angle. If an object moves too slowly or too fast, the sensor may not detect it accurately. Sensitivity to the Environment: PIR sensors can be influenced by environmental conditions such as temperature, humidity, and other heat sources. Sudden changes in temperature or heat sources moving around the sensor can cause false alarms. Limited Range: PIR sensors typically have a limited detection range, often around 5-10 meters. This may not be enough for some applications that require motion detection over a larger area.

Device Integration

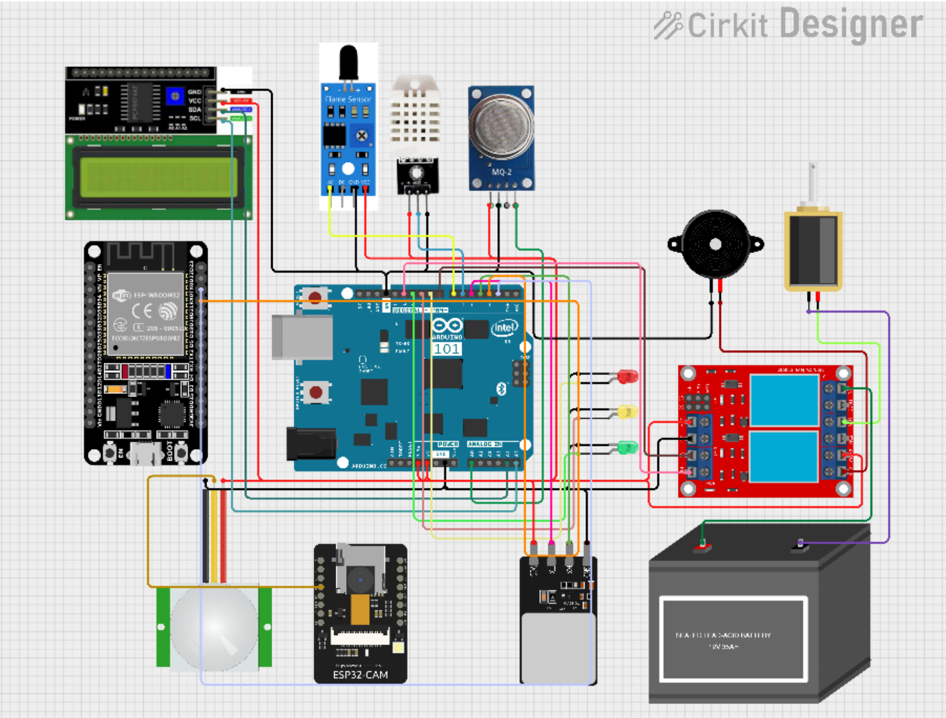

Figure 7 Integration

Based on the picture above, the Arduino UNO is the data processing brain in the tool being made. Input to the device includes a fire sensor connected to pin 7, a DHT22 sensor connected to pin 6, an MQ2 sensor connected to pin A0, a fingerprint sensor connected to pin 4 and pin 5, a PIR sensor connected to pin IO13 on the ESP32 cam. Pin 9, pin 10, and pin 11 initialize to control the LED. The I2C module on the 16x2 LCD is connected to pins A4 and A5. The buzzer as a warning is connected to pin 1 on the relay. The door lock solenoid as a door lock is connected to pin 2 on the relay. The 2-channel relay module is connected to the Arduino UNO where VCC and ground are connected to ground and 5v on the Arduino UNO, pin 1 of the relay is connected to pin 8 on the Arduino UNO to control the buzzer, and pin 2 of the relay is connected to pin 12 on the Arduino UNO to control the door lock solenoid. Pin 2 and pin 3 on the Arduino UNO are connected to the RX and TX pins on the ESP32 for serial communication. The data obtained from the sensor will be processed then the Arduino will provide output on the 16x2 LCD which will display whether the condition is dangerous or not, a buzzer will light up if there is an indication of fire, an LED light will light up based on existing conditions, and the door lock solenoid will open if the presence of verified fingerprints or the required conditions are met. The Arduino UNO will send data from the sensor to the ESP32 serially, then the ESP32 which is connected to an internet connection will send the data to the database on the website.

Table 4 Integration Indicators

No.	Parameter	Success Indicators	Test Result
1.	LCD 16x2	Displays the condition of whether there is a fire or not.	The test results were declared successful because they could display the conditions in clear and easy to read letters
2.	Flame Sensor	Can detect fire well.	The test results were declared successful because it could detect when there was a fire and send a signal if the fire was detected.
3.	Smoke Sensor	Can detect gas/smoke well.	The test results were declared successful because it could detect gas/smoke and send a signal if the detected gas/smoke exceeded the threshold.
4.	Temperature Sensor	Can detect the surrounding temperature well.	The test results were declared successful because it could detect the surrounding temperature and would send a signal if the temperature exceeded the specified threshold.
5.	Fingerprint	Can verify fingerprints well.	The test result is declared successful because it can verify the fingerprint properly and will send a signal to the Arduino to unlock the door.
6.	Sensor PIR	Can detect movement well.	The results of the test are said to be successful because they can detect movement and will send a signal if movement is detected.
7.	Relay 2 channel	Can perform switching well.	The results of the test are said to be successful because the relay will switch when it gets a signal from Arduino.
8.	Buzzer	Active when fire conditions are met.	The test results were declared successful because the buzzer will turn on when the fire sensor, temperature sensor and smoke sensor detect fire, high temperature and excessive smoke.
9.	Solenoid door lock	Can lock and unlock when getting a signal.	The results of the test were declared successful because the door lock will lock and open when the relay switches when it gets a signal from Arduino.
10.	ESP32	ESP32 as a component to send data obtained from Arduino to the database.	The test results were declared successful because the ESP32 was able to send data from Arduino to the database when connected to the internet.
11.	ESP32 CAM	The ESP32 CAM is used to take pictures if conditions are met.	The test results were declared successful because the ESP32 CAM was able to take pictures when given a command and when the PIR sensor detected movement then sent it to Telegram as a notification.
12.	Arduino UNO	Arduino UNO as the brain of the device.	The test results were declared successful because the Arduino UNO was able to receive data from the input, process the data, and produce output.

This study showcases the dual functionality of IoT-based security systems, resonating with existing literature on IoT's transformative potential. IoT technologies have been widely recognized for enhancing safety in various sectors. For instance, Al-Fuqaha et al. (2015) highlight IoT's ability to facilitate real-time monitoring and automation in smart environments. Similarly, Kumar and Patel (2014) demonstrated that IoT systems provide efficient data collection and immediate responsiveness, which are crucial for security applications.

By integrating this system into an academic framework, the research aligns with studies that advocate for technology-enabled learning. For example, Trilles et al. (2017) emphasize the role of IoT in providing hands-on learning opportunities and helping students develop skills aligned with industrial needs. This research furthers that notion by proving that security systems can double as educational tools, fostering student innovation.

The findings confirm the efficacy of IoT in enhancing safety. Real-time alerts, automated data analysis, and continuous surveillance are among the features that make IoT systems superior to traditional methods. As Gubbi et al. (2013) supported, IoT systems provide seamless integration of sensors and devices, enabling efficient and proactive responses to security threats. The research at Makassar Aviation Polytechnic validates this by demonstrating improved security through real-time monitoring and prompt incident reporting. This study underscores how IoT-based systems can revolutionize learning methodologies. The system's integration into the curriculum allowed students to work directly with IoT devices, fostering experiential learning. Studies like Zhang et al. (2019) support this approach, indicating that IoT technologies can effectively teach automation, programming, and system integration. This research prepares students for IoT-related challenges in aviation and beyond by exposing them to real-world applications.

The scalability of the designed system reflects its potential for broader applications. Future expansions involve integrating AI for predictive analytics or expanding the system to cover larger areas. This aligns with the work of Perera et al. (2014), who emphasize the adaptability of IoT systems across various domains, from healthcare to smart cities. In conclusion, this research contributes to understanding IoT's role in addressing dual objectives: enhancing security and advancing education. Demonstrating the successful implementation of an IoT-based security camera system at Makassar Aviation Polytechnic lays the foundation for further exploration and application in similar contexts.

CONCLUSION

Based on the results of the research and testing of security camera equipment, the author provides the following conclusions. This research highlights the critical role of IoT-enabled security cameras in enhancing safety, fostering practical automation learning, and driving innovation at Makassar Aviation Polytechnic, with broad potential for scalable applications in education and beyond. The research aims to design and implement IoT-based security cameras for smart rooms at Makassar Aviation Polytechnic, using a strategy that includes needs analysis, system design, prototype development, educational integration, performance evaluation, and scalability optimization to enhance security and foster hands-on automation learning. The research revealed that IoT-based security cameras are highly effective in improving the safety and monitoring of smart rooms at Makassar Aviation Polytechnic. The system provided real-time surveillance, streamlined security management, and quick incident detection, significantly enhancing the overall safety framework. Additionally, integrating these technologies into the curriculum proved an impactful learning tool, allowing students to gain hands-on experience with IoT systems, automation processes, and network protocols. This dual-purpose approach demonstrated the potential for IoT technology to address practical security challenges and serve as an innovative educational resource. This research has provided new insights into the dual utility of IoT-based systems, demonstrating that they can simultaneously enhance security measures and serve as interactive educational tools. It highlights how IoT technologies can be tailored to address the specific needs of intelligent environments, integrating seamlessly into operational and instructional frameworks. The study contributes to the growing body of knowledge in IoT applications by illustrating the practical implementation of IoT-enabled security cameras in an academic setting. It bridges the gap between theoretical IoT concepts and real-world applications, offering a scalable model for educational institutions seeking to integrate advanced technologies into their infrastructure. This research advances the field by showcasing how IoT systems can support interdisciplinary objectives, combining security, automation, and education. It provides a roadmap for future studies on integrating IoT technologies in other domains, such as healthcare, industrial automation, and innovative city development, further reinforcing IoT's versatility and transformative potential. The writer hopes that readers will recognize the transformative potential of IoT-based technologies as tools for enhancing security and as powerful educational resources. By embracing the findings of this research, readers are encouraged to explore innovative applications of IoT in their respective fields, drive advancements in intelligent systems, and contribute to technology integration in solving practical and educational challenges.

REFERENCES

Ahmad, S., Ali, M., & Khan, M. (2020). Smart Classroom Automation and Security Using Internet of Things (IoT). *Journal of Educational Technology & Systems*, 48(2), 153-161. https://doi.org/10.1177/0047239520911853

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347-2376.

Anantama, A., Apriyantina, A., Samsugi, S., & Rossi, F. (2020). Tool for Monitoring the Amount of Electrical Power Used in Electronic Devices based on Arduino UNO. *Journal of Embedded Technology and Systems*, 1(1), 29-34.

Ardiansyah, M. F., & Rosyani, P. (2023). UI/UX design of Inorganic Waste Processing Applications using the Design Thinking method. logic: journal of computer science and education, 1(4), 839-853.

Arif, A., & Mukti, Y. (2017). Website Design for State Junior High Schools (SMP) 8 cities of Pagar Alam. Betrik Scientific Journal: Information and Computer Technology, 8(03), 156-165.

Arduino, S. A. (2015). Arduino. Arduino LLC, 372.

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. Interacting with computers, 23(1), 4-17.

Burange, A. W., & Misalkar, H. D. (2015, March). Review of the Internet of Things in development of smart cities with data management & privacy. In 2015 International Conference on Advances in Computer Engineering and Applications (pp. 189-195). IEEE.

Buchari, M. Z., Sentinuwo, S. R., & Lantang, O. A. (2015). Design a 3-dimensional animated video for motor vehicle testing mechanisms in transportation, culture, tourism, communication, and information services. Journal of Informatics Engineering, 6(1).

Cameron, N. (2023). ESP32-CAM Camera. In ESP32 formats and communications: application of communications protocols with esp32 microcontroller (pp. 447-488). Berkeley, CA: Apress.

Chaturvedi, A., Kumar, P., & Rawat, S. (2016, October). Proposed novel security system based on passive infrared sensors. In 2016 International Conference on Information Technology (InCITe)-The Next Generation IT Summit on the Internet of Things: Connect your Worlds (pp. 44-47). IEEE.

Chaudry, A. M. (2020). Using Arduino Uno microcontroller to create interest in physics. The Physics Teacher, 58(6), 418-421.

Fathulrohman, Y. N. I., & Saepulloh, A. (2019). Temperature and humidity monitoring tool using Arduino Uno. Journal of Management and Information Engineering (JUMANTAKA), 2(1).

Gall, M. D., & Borg, W. R. (1989). Educational research. A guide for preparing a thesis or dissertation proposal in education. Longman, Inc., Order Dept., 95 Church Street, White Plains, NY 10601 Stock No. 78164-6.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.

Hesti, E. (2012). Design a moving monitoring camera system with a pir sensor (transmitter). teliska, 4(3).

Jain, A., Gupta, R., & Sharma, S. (2021). Design and implementation of an IoT-based smart security system for intelligent environments. *Journal of Internet of Things and Smart Technologies*, 5(3), 112-121. https://doi.org/10.1016/j.iot.2021.01.007

Junaidi, A. (2015). Internet of things, history, technology and applications. Scientific Journal of Applied Information Technology, 1(3).

Kalengkongan, T. S., Mamahit, D. J., & Sompie, S. R. (2018). Design of a Noise Detection Tool Based on Arduino Uno. Journal of Electrical and Computer Engineering, 7(2), 183-188.

Kumar, S., & Patel, P. (2019). IoT-based surveillance system for smart classrooms. *International Journal of Smart Education and Technology*, 6(4), 215-222. https://doi.org/10.1016/j.ijsmet.2019.05.004

Kumar, D., & Patel, D. R. (2014). A survey on Internet of Things: Security and privacy issues. *International Journal of Computer Applications*, 90(11), 20-26.

Kurniawan, M. I., Sunarya, U., & Tulloh, R. (2018). Internet of Things: Home Security System based on Raspberry Pi and Telegram Messenger. ELKOMIKA: Journal of Electrical Energy Engineering, Telecommunications Engineering, & Electronics Engineering, 6(1), 1.

Koroy, A. M. S., Mandar, G., & Muhammad, A. H. (2020). Design and Build a Home Door Security System Using ESP32-CAM. Journal of Informatics Engineering (J-Tifa), 3(2), 32-36.

Latifa, U., & Saputro, J. S. (2018). Design of an Arduino Uno based robot arm gripper using the Labview interface. Barometer, 3(2), 138-141.

Louis, L. (2016). working principle of Arduino and u sing it. International Journal of Control, Automation, Communication and Systems (IJCACS), 1(2), 21-29.

Maulani, G., Septiani, D., & Sahara, P. N. F. (2018). Design and construction of the Maintenance Facility Inventory information system at Pt. PLN (Persero) Tangerang. ICIT J, 4(2), 156-167.

Nurhayati, A. N., Josi, A., & Hutagalung, N. A. (2017). Design of an application for selling and purchasing goods at the Kartika Samara Grawira Prabumulih cooperative. Journal of Technology and Information, 7(2), 13-24.

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context-aware computing for the Internet of Things: A survey. *IEEE Communications Surveys & Tutorials*, 16(1), 414-454.

Purnamasari, A. I., & Setiawan, A. (2019). Development of Passive Infrared Sensor (PIR) HC-SR501 with ESP32-CAM Microcontrollers Based on Internet of Things (IoT) and Smart Home as Motion Detection for Housing Security. Proceedings of SISFOTEK, 3(1), 148-154.

Tempongbuka, H., Allo, E. K., & Sompie, S. R. (2015). Design and Build a Home Security System Using PIR (Passive Infrared) Sensors and SMS as Notifications. Journal of Electrical and Computer Engineering, 4(6), 10-15.

Trilles, S., González-Pérez, A., & Huerta, J. (2017). A comprehensive IoT learning system based on real IoT devices. *Future Internet*, 9(4), 69

Rachmawati, A. (2023). monitoring chili plants from caterpillar pests using PIR and ESP32 CAM sensors (Doctoral dissertation, Indonesian Digital Technology University).

Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. The Internet Society (ISOC), 80(15), 1-53.

Royce, W. W. (2021). Managing the development of large software systems (1970).

Ruuhwan, R., Rizal, R., & Kurniawan, R. (2020). Motion detectors use pir sensors for SMS-based room security systems. Pamulang University Informatics Journal, 5(3), 281-287.

Singh, A., & Gupta, S. (2022). IoT-based security camera design for educational institutions. *International Journal of Security and Privacy in Smart Environments*, 7(1), 49-57. https://doi.org/10.1016/j.ijspse.2022.02.003

Wahid, A. A. (2020). Analysis of the waterfall method for information system development. J. Information Sciences. and Manaj. STMIK, no. November, 1(1), 1-5.

Yurita, I., Ramadhan, M. K., & Candra, M. (2023). The Influence of Technological Progress on the Development of Cybercrime (a case study of phishing as a digital security threat). Legalita Law Journal, 5(2), 143-155.

Zhang, D., Li, X., & Shi, W. (2019). IoT-enabled education: Opportunities and challenges. *IEEE Internet of Things Journal*, 6(5), 7535-7543

Zuhri, K., & Ikhwan, A. (2020). Telegram-Based Dual Security System Design Using ESP32-CAM Microcontroller. Journal of Technology and Informatics (PAUSE), 1(2).