Jurnal Ilmu Pendidikan (JIP)
Vol. 31, Issue 2, December 2025, pp. 343-353 ISSN: 0215-9643 e-ISSN: 2442-8655

Analysis of Conceptual Understanding of Aviation Security (AVSEC) Topic Course with Science, Technology, Engineering, and Mathematics (STEM) Approach: Study of the Perimeter Introdure Detection System (PIDS) Using Arduino and Pir Sensor

Ahmad Musadek* Bambang Bagus Harianto, Maulana Anifa Silvia, Faoyan Agus Furyanto, Didi Hariyanto, Lady Silk Moonlight

Politeknik Penerbangan Surabaya, Jl. Jemur Andayani I No.73, Siwalankerto, Surabaya, 60236, Indonesia
*ahmad.dzadek@gmail.com**
** corresponding author*

ARTICLE INFO

Article history
Received August 9, 2025
Revised Nov 18, 2025
Accepted Dec 30, 2025

Keywords
STEM
Aviation Security
PIDS, Arduino
Passive Infrared Receiver

ABSTRACT

This study aims to analyze students' conceptual understanding of the "Aviation Security" (AVSEC) course, focusing on the topic of Perimeter Intruder Detection System (PIDS) using the Science, Technology, Engineering, and Mathematics (STEM) approach. This study uses a quasi-experimental design with pre-test and post-test approaches to evaluate the effectiveness of STEM approaches in improving students' conceptual understanding. A total of 25 cadets from the MTU study program, Surabaya Aviation Polytechnic, became the subject of the research. The instruments used include conceptual comprehension tests, observation sheets, questionnaires, and in-depth interviews. The results of data analysis using the Paired Sample T-Test showed that there was a significant increase in student understanding after the application of STEM methods. The average value of the difference between the pre-test and the post-test was -17.750 with a standard deviation of 4.665, and a significance level of 0.000, indicating a significant increase in understanding. The 95% confidence interval for the mean difference is between -19, which 720 to -15,780. The PIDS system was developed using the Research and Development (R&D) method, while the development of hardware and software followed the Waterfall approach. The results of this research make an important contribution to the development of STEM-based learning methods in the field of aviation safety, especially on the topic of PIDS.

I. Introduction

Aviation Security (AVSEC) is one of the key elements in maintaining global aviation safety. With the increasing volume of commercial flights, airport security is a top priority to prevent illegal acts such as terrorism, smuggling, and sabotage (Bashir et al., 2019). The airport perimeter is a critical area vulnerable to threats, as it serves as the first line of defense in the airport security system. In this context, the Perimeter Intruder Detection System (PIDS) plays an essential role in detecting and responding to potential threats and intrusions in the airport's vicinity. Implementing an effective intruder detection system not only enhances the security of airport facilities but also reduces risks to public safety (Kuo et al., 2019).

Recent studies emphasize that aviation security faces increasing challenges due to cyber and physical intrusions targeting airport infrastructures. The integration of digital surveillance, artificial intelligence (AI), and real-time analytics is therefore essential to strengthen operational safety. Research by Ojo-Oba (2025) highlights that the complexity of cyber threats, such as ransomware, GPS spoofing, and data breaches, has intensified the need for multidisciplinary and technologically adaptive aviation security systems. This finding reinforces the importance of integrating both physical and cyber-intrusion detection mechanisms within AVSEC frameworks.

Modern perimeter security systems can detect suspicious movements in real time and provide early warnings to airport security personnel. However, managing extensive and open perimeter areas requires reliable, integrated, and adaptive systems, as threats may emerge from multiple vectors and at unpredictable times. Therefore, the implementation of advanced Perimeter Intrusion Detection Systems (PIDS), enhanced with Internet of Things (IoT) connectivity, offers an effective solution for detecting and mitigating suspicious activity in

http://dx.doi.org/10.17977/um048v31i2p343-353

perimeter areas (Voronkin & Lushchin, 2023). Recent innovations have shown significant progress in IoT-based detection through automation and AI-assisted monitoring. For instance, Villegas-Ch & García-Ortiz (2023) developed an AI-integrated perimeter monitoring framework capable of real-time authentication and movement analysis in critical infrastructure environments, demonstrating the potential for more accurate and efficient PIDS in aviation security contexts. As an integral component of Aviation Security (AVSEC), comprehensive knowledge of PIDS is essential for aviation security practitioners, underscoring the importance of effective learning approaches for AVSEC students to master this technology (Görgülü Arı & Meço, 2021).

Technological developments in security systems have advanced rapidly, particularly over the past decade. In the field of aviation security, modern tools such as Passive Infrared Receiver (PIR) sensors, radar, and thermal cameras, combined with artificial intelligence (AI)-based systems, have significantly transformed how airports and related facilities maintain perimeter integrity (Johnson et al., 2022). Using PIR sensors and microcontrollers such as Arduino, the PIDS system can detect suspicious movements and alert security personnel via an IoT network. This enables more efficient and responsive security management at both local and global levels (Gilder & O'Rourke, 2018).

The Science, Technology, Engineering, and Mathematics (STEM) approach is highly relevant to aviation safety, particularly in the instruction of technological systems such as PIDS. STEM-based learning encourages students to engage in interactive integration of theory and practice by designing, developing, and testing intelligent security systems. The integration of microcontrollers and sensors in learning activities enables students to gain direct experience in implementing real-world technological solutions (Achzab et al., 2018). Recent findings by Houichi et al. (2025) confirm that STEM-oriented education, when applied in IoT and security system design, enhances learners' practical problem-solving abilities and digital readiness, particularly in vocational education settings where applied learning is essential.

STEM approaches not only enhance students' theoretical understanding but also equip them with the technical and analytical skills demanded in the modern workforce. In the context of vocational education, such approaches provide a strong foundation for developing both conceptual and practical expertise, ultimately preparing students to meet the professional demands of the aviation security sector (Wawan et al., 2022). Therefore, integrating IoT-based technologies, such as Arduino and PIR sensors, into AVSEC education not only strengthens learning outcomes but also aligns academic practices with real-world aviation security challenges.

A. Theoretical Foundations

1) STEM-Based Learning Theory (Revised)

STEM-based learning (Science, Technology, Engineering, and Mathematics) is an educational approach that integrates these four disciplines to equip students with the skills needed in the modern era. Some of the theoretical foundations that support STEM-based learning are:

2) Constructivist Theory

Learning is an active process in which students build knowledge from experience and interaction with the surrounding environment (Kelley & Knowles, 2016). In STEM contexts, students engage directly in projects and experiments to discover new concepts through practical experience.

3) Project-Based Learning Theory

STEM is also rooted in the PBL approach, which encourages students to complete real projects that require integrating various disciplines. This helps students understand the interconnectedness of the discipline and its application in daily life (Mpofu, 2019). Project-based learning has been recognized as a vital pedagogical strategy in vocational education, supporting problem-solving, collaboration, and creativity. Recent research by Triono Ahmad et al. (2023) confirms that project-based learning remains a leading model in vocational education, fostering higher-order thinking and practical competence through integrated, technology-supported instruction.

4) Interdisciplinary Approach

STEM-based learning integrates multiple disciplines to address real-world problems (Takeuchi et al., 2020). This approach promotes the synthesis of knowledge across scientific and technological domains, allowing learners to connect theory with practice. The SOAR model introduced by Seo et al. (2024) demonstrated how interdisciplinary project-based learning strengthens collaboration, adaptability, and multidisciplinary problem-solving, key attributes for future engineers and technical professionals.

5) 21st Century Skills Theory

STEM aims to develop the critical thinking, creativity, communication, and collaboration skills needed in an increasingly digital and connected world of work (Ortiz-Revilla et al., 2021). Recent studies emphasize that STEM integration in vocational contexts equips students with not only technical but also employability competencies. According to Akmal et al. (2025), integrating STEM and project-based learning significantly enhances vocational students' competence, motivation, and readiness for employment through holistic learning experiences that combine theory and practice.

B. Aviation Security (AVSEC)

Aviation Security (AVSEC) is a system designed to protect passengers, crew, and aviation assets from threats such as terrorism and sabotage. This system relies on advanced technologies, such as Advanced Imaging

Technology (AIT) and risk-based systems, to detect threats more accurately (Karoly, 2017). The main challenges of AVSEC are high operational costs and security effectiveness, which are often questioned despite the significant investments made (Stewart & Mueller, 2018).

In recent years, aviation security has evolved significantly with the integration of advanced digital infrastructures and Internet of Things (IoT)-based monitoring systems to improve real-time detection and situational awareness. As airports transition into innovative ecosystems, cyber and physical threats have become more complex, necessitating adaptive and resilient security architectures. According to Mizrak & Reyhan Akkartal (2024), implementing multi-layered cybersecurity strategies, including real-time threat detection, encryption protocols, and user training, is essential to maintaining safety and operational continuity in global air transport. These findings highlight that AVSEC systems must not only rely on traditional screening mechanisms but also integrate digital intelligence and IoT-based technologies to counter increasingly sophisticated threats effectively.

1) Perimeter Intruder Detection System (PIDS)

The Perimeter Intruder Detection System (PIDS) is a security system designed to detect and warn of intrusions around the boundaries of a protected area, such as an airport. Modern PIDS technology leverages intelligent detectors, information networks, and software to minimize false alarms and improve detection accuracy (Teixidó et al., 2021).

Recent developments have integrated Internet of Things (IoT) architectures, artificial intelligence (AI), and sensor fusion into PIDS frameworks to enhance situational awareness and detection precision. For example, Pitafi et al. (2023) introduced a machine-learning-driven PIDS prototype that combines DHT22 temperature sensors, vibration modules, and Mini PIR motion sensors, all controlled by an Arduino. The system achieved over 94.9% detection accuracy using an improved DBSCAN clustering algorithm (ST-DBSCAN) for real-time anomaly detection in perimeter security. This innovation demonstrates how intelligent IoT and AI integration can significantly improve the reliability and responsiveness of PIDS, particularly in critical infrastructures such as airports.

2) Method Waterfall

The Waterfall method is a classic, systematic, and sequential model used in software development that starts with analysis, design, coding, and testing (Pressman, 2015). This method is suitable for developing security systems such as PIDS, as it requires clear stages in the design and implementation of the technology.

In modern IoT-based security systems, the Waterfall approach remains relevant for projects that demand structured documentation and well-defined development phases. Recent research by Jaelani et al. (2023) demonstrated the integration of the Waterfall Software Development Life Cycle (SDLC) in the creation of an IoT-based Smart Street Lighting System using the Laravel framework. The study showed that applying the Waterfall model improved the efficiency, security, and responsiveness of IoT software by ensuring a structured flow from requirement analysis to testing. This finding supports the continued use of the Waterfall methodology in security-oriented system development, including PIDS, where reliability and precision are critical.

C. Passive Infrared (PIR) Sensor and PIR Sensor Microcontroller (Revised)

Passive Infrared (PIR) sensors detect human movement using infrared radiation naturally emitted by the human body. In the context of the Perimeter Intruder Detection System (PIDS), PIR sensors are integrated with microcontrollers such as Arduino to detect suspicious activity along airport perimeters (Irianto & Novianti, 2020). These sensors convert changes in infrared energy into electrical signals, enabling systems to detect motion without physical contact.

Microcontrollers such as the ESP32-Cam are equipped with Wi-Fi and Bluetooth connectivity, making them ideal for Internet of Things (IoT) applications in PIDS systems (Rahmawati et al., 2022). The integration of IoT and microcontrollers enhances real-time monitoring capabilities. It enables automatic alerts via connected networks, which is essential for security systems in high-risk environments such as airports.

Recent innovations in IoT-based security frameworks have underscored the growing importance of integrating PIR sensors with intelligent microcontroller platforms. Research by Annalakshmi (2023) introduced the CommandFence system, an IoT-based perimeter monitoring model that integrates PIR sensors, NodeMCU, and ESP32-CAM for intrusion detection. This system not only detects unauthorized movement but also captures visual confirmation and sends real-time alerts via Telegram integration. Such advancements highlight how IoT-based PIR and microcontroller systems can improve accuracy, reduce false alarms, and support scalable applications in perimeter security including aviation security infrastructures.

II. Method

This study uses a modified Research and Development (R&D) approach to analyze students' conceptual understanding of the "Aviation Security" (AVSEC) course, focusing on the Perimeter Intruder Detection System (PIDS) using the Science, Technology, Engineering, and Mathematics (STEM) approach. This research is carried out in several stages, including planning, development, implementation, and evaluation.

A. Research Design

The research population is students of the DIII Air Transportation Management Study Program at the Surabaya Aviation Polytechnic who take AVSEC courses in the odd semester of the 2023/2024 academic year. The research sample was selected using purposive sampling, comprising 24 students who participated in STEM-based learning on PIDS. Tool design is a critical stage that ensures the tool or product developed functions according to the needs and specifications determined. This process begins by identifying user needs and determining the necessary technical specifications, such as movement-detection capabilities, and by sending notifications to the perimeter security system. After that, selecting the right components, such as the PIR sensor, ESP32-Cam microcontroller, and monitoring applications like Blynk, is a key step to ensure that every part of the system functions optimally. Diagram and schematic block designs are also necessary to provide a visual representation of how the components interact and to ensure proper, efficient connections. Once all the system's elements have been identified and designed, simulations are conducted to test the system's functionality before physical prototyping. With a mature design, the implementation process becomes more directed, with minimal errors, and allows the system to work efficiently to detect intruders and maintain airport perimeter security.

B. Population and Sample

The research population is students of the DIII Air Transportation Management Study Program at the Surabaya Aviation Polytechnic who take AVSEC courses in the odd semester of the 2023/2024 academic year. The research sample was selected using purposive sampling, comprising 24 students who participated in STEM-based learning on PIDS.

C. Research Instruments

The instruments used in this study include:

1) Conceptual Comprehension Test

This test consists of 25 multiple-choice questions designed to evaluate theoretical comprehension and practical applications of PIDS before and after learning.

2) Observation Sheet

This sheet is used to record student engagement during STEM-based learning. Aspects observed include involvement in discussions, problem-solving abilities, and technical skills with Arduino and PIR sensors.

3) Questionnaire

This questionnaire collects data on students' perceptions of the effectiveness of STEM approaches and the difficulties they face in learning.

4) In-Depth Interviews

Interviews are conducted with several students to gain deeper insight into their learning experiences and the factors that affect their conceptual understanding.

Table 1. Prosedur Penelitian

Phase	Activities
Planning Stage	The researcher identified the key concepts to be taught in the PIDS topic as well as designed a STEM-based learning module that involved the use of Arduino and PIR sensors. Research instruments such as conceptual comprehension tests, observation sheets, questionnaires, and interview guides are compiled and validated by experts in the field of aviation education and safety.
Development Stage	The learning modules that have been designed are implemented in the form of practicum in a laboratory equipped with Arduino devices and PIR sensors. Students have explained the basic concepts of PIDS as well as tutorials on how to use related technology devices.
Implementation Stage	Students take part in learning with a STEM approach, where they are required to design and implement a PIDS system using Arduino and PIR sensors. This learning process lasts for four weeks, with each session lasting 2 hours.
Evaluation Stage	After the learning is complete, students are given a post-test to measure their improvement in conceptual understanding. Data from observation sheets, questionnaires, and interviews were analyzed to complement the quantitative results of the comprehension test. The pre-test and post-test results were analyzed using paired t-tests to determine whether there was a significant improvement in students' conceptual comprehension.

D. Research Procedures

This research is carried out through four main stages, namely planning, development, implementation, and evaluation. In the planning stage, researchers identified key concepts in the Perimeter Intruder Detection System (PIDS) and designed STEM-based learning modules that use technologies such as Arduino and PIR sensors. In addition, aviation education and safety experts validate research instruments, including conceptual comprehension tests, observation sheets, questionnaires, and interview guides, to ensure their accuracy. During the development stage, the designed modules are implemented as a practicum in laboratories equipped with these technologies. Students receive an explanation of the basic concepts of PIDS and tutorials on the use of technological devices.

Furthermore, the implementation phase lasts four weeks, with two-hour learning sessions each week, during which students actively participate in designing and implementing the PIDS system using Arduino and PIR sensors. The final stage is evaluation, during which students are given post-tests to assess their conceptual understanding following STEM-based learning. Data from observation sheets, questionnaires, and interviews were also analyzed in depth to complement the quantitative results obtained from comprehension tests. Paired t-tests were used to determine whether there was a significant improvement in student understanding.

E. Design/Coding

The design and coding stage is a critical phase that translates the system design into code that can be operated by hardware. In this stage, the formulated design is implemented in C++, a language specifically designed to control ESP32 components. The Arduino IDE became the primary tool in this process, in which the researcher programmed pin settings, sensor configurations, and logic to enable the system to function as planned. Once the coding process is complete, a thorough system test is conducted to detect potential errors and ensure all functions are running correctly. Another essential part is the integration with the Blynk app, which enables real-time monitoring and control of the system from Android devices. With Blynk, users can easily monitor security systems, receive live notifications, and remotely interact with devices, making the system more responsive and easier to operate. This process ensures that the entire suite from design to execution runs efficiently and effectively, with an emphasis on accuracy and reliability in real-world applications.

F. Testing

Researchers conducted live field tests to evaluate the performance of passive infrared (PIR) sensors and camera modules attached to security devices. This test also includes an evaluation of the Blynk application integrated with the system to ensure all components function as expected. In this testing process, researchers focus not only on basic functionality but also on identifying potential errors that may arise during operation.

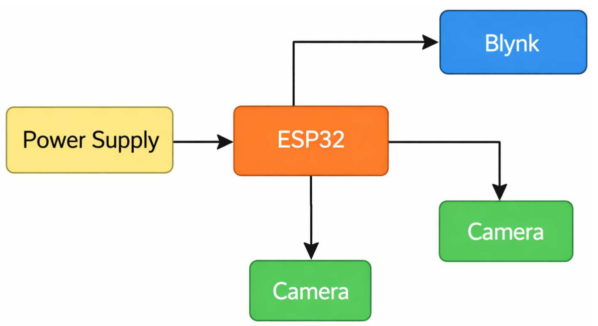

Fig. 1. Block diagram tool

The results of these tests provide data to correct any errors, enabling further optimization of the system. In addition, the test aims to verify the system's effectiveness in detecting movement using PIR sensors, measure the sensor's effective range, and determine the optimal angle of capture for detecting movement. Testing of the camera module is also carried out to ensure the camera's ability to capture images and videos accurately by the instructions provided through the Blynk application. With this series of in-depth tests, researchers can ensure that the security tools they develop are optimized and conform to the specifications for which they were designed.

G. Product Validation Questionnaire

A questionnaire is an instrument that asks respondents to answer based on what they know and experience. The questionnaire in this study aims to elicit assessment, criticism, and suggestions from experts on the product.

Table 2. Table Scale Likert

No.	Category	Shoes
1.	Strongly Agree	4
2.	Agree	3
3.	Disagree	2
4.	Strongly disagree	1

Table 2 shows the Likert scale categories in the product validation questionnaire, with a score range of 4 (strongly agree), 3 (agree), 2 (disagree), and 1 (strongly disagree). The score obtained from the questionnaire will be converted to a percentage specified by the following formula:

$$\textbf{\textit{Indeks}} = \frac{score\ obtained}{maximum\ score}\ x\ 100\%$$

After the questionnaire results are distributed to assess product validity and the validity is determined using the formula above, the percentage results are adjusted using the criteria in Table 3.

Table 3. Product Validity Index

No.	Index	Score
1.	Very worth using with little revision	75% - 100%
2.	Quite feasible to use with revision	50% - 75%
3.	Less usable with many revisions	25% - 50%
4.	Not fit for use	0% - 25%

Here are some examples of instrument items in the 4-option Likert scale based on the indicators already mentioned. A rating scale follows each instrument item: Strongly Disagree (STS), Disagree (TS), Agree (S), and Strongly Agree (SS), presented in the appendix.

III. Results and Discussion

This research develops the Perimeter Intruder Detection System (PIDS) tool to make it easier for Aviation Security (AVSEC) officers to monitor the airport perimeter. Using the Blynk application, this tool can automatically send notifications when people enter a restricted area. In addition, this research focuses on improving students' conceptual understanding of PIDS through the Science, Technology, Engineering, and Mathematics (STEM) approach in Aviation Security (AVSEC) learning.

A. Analyzes

The results of the needs analysis indicate that the desired security system must meet several key criteria. First, the system must be able to detect the movement of living things, especially humans, using PIR sensors. Second, this system must be connected to the Blynk application, enabling users to receive automatic notifications when suspicious movements are detected. Third, the system also needs to provide security-monitoring features, including video streaming and live shooting, accessible via the Blynk application. With these features combined, the system will provide more effective, responsive security for monitoring restricted areas.

1) Student Conceptual Understanding

After the STEM-based learning on PIDS, the results of the conceptual comprehension test showed a significant improvement. Data were obtained through pre- and post-test measures, observation sheets, and questionnaires.

The results of the descriptive analysis in the paired samples test (Paired Samples Statistics) showed that the average value before treatment (Pre) was 56.83, while the post-treatment value (Post) increased to 74.58. With a sample of 24 students, the average increase was 17.75 points. This increase indicates that the STEM approach positively affects students' understanding.

The standard deviation before treatment was 9.03, while after treatment it increased to 11.21, indicating that the data are more dispersed. The means before and after treatment were 1.84 and 2.29, respectively. To ensure that this difference was statistically significant, a t-test was conducted for paired samples (paired samples t-test), which indicated a substantial improvement in students' conceptual understanding.

2) Correlation Results

The paired-samples correlation test showed a strong correlation between the pre- and post-treatment values ($r = 0.916$). This value is close to 1, indicating that the change in grades after learning is closely related to the grades before learning. A significance value (p-value) of 0.000 indicates that this correlation is statistically significant ($p < 0.05$), so it can be concluded that STEM-based learning treatment has a consistent effect on improving student understanding.

3) Paired t-test

The t-test results showed a significant difference between the pre-test and post-test scores. The mean difference is -17.75 with a standard deviation of 4.665. The calculated t-value is -18.641, with a degree of freedom (df) of 23 and a p-value of 0.000, indicating that this difference is statistically significant. This shows that the STEM approach is effective in increasing students' conceptual understanding of PIDS topics.

4) Student Engagement Observation

Based on observations, students showed high involvement in practicum activities. Students are very enthusiastic about designing and implementing PIDS systems using Arduino and PIR sensors. Although some students face technical challenges, most can apply the theory they have learned to practice. The observation assessment graph shows that overall student engagement is rated good, with an average score above the threshold.

5) Student Perception

The questionnaire results showed that students' perception of AVSEC learning with a STEM approach was very positive. The Likert scores from students indicate that all statements have an average score above 4.0. This positive perception confirms that the STEM approach is successful in providing a more interactive and applicable learning experience. The statement regarding the integration of technology in PIDS learning received the highest score (4.8), indicating appreciation for the use of Arduino and PIR sensors in learning.

6) Interview Results

In-depth interviews with students showed that STEM approaches that integrate theory and practice help improve their understanding. Students feel they are better able to relate theoretical concepts to practical applications in the real world, especially in developing PIDS using Arduino and PIR sensors. They also think that the hands-on learning approach provides a deeper understanding of the material. Some students identified technical challenges with the device, but with more intensive guidance and training, they managed to overcome them.

The results of this study show that the STEM approach is very effective in increasing students' conceptual understanding of PIDS topics. Research shows that hardware-based learning methods, such as Arduino, can significantly improve students' ability to apply theory to practice (Gilder & O'Rourke, 2018). This aligns with recent studies showing that integrating STEM and IoT-based learning media can enhance both conceptual mastery and technical competence. According to Hamid et al. (2022), the implementation of IoT-based learning media using Arduino and sensors within a STEM framework improved student learning outcomes by over 70%, demonstrating the effectiveness of such hands-on, technology-driven pedagogy in applied science education.

The success of STEM approaches can be attributed to the integration of theory and practice, which enables students to see firsthand how the concepts they learn can be applied in the real world (Wawan et al., 2022). Additionally, the use of devices such as Arduino and PIR sensors provides an efficient, hands-on experience that develops technical skills and conceptual understanding (Achzab et al., 2018). This is supported by the findings of Feng & Hou (2023), who emphasized that integrating STEM-based vocational education fosters industry-relevant competencies by combining theoretical

Jurnal Ilmu Pendidikan (JIP)
Vol. 31, Issue 2, December 2025, pp. 343-353

knowledge with direct, experiential learning, which is critical for preparing graduates to meet real-world technical demands.

However, the technical challenges faced by some students highlighted the need for additional support in using technological devices to ensure that all students can follow the learning process effectively. Overall, this study demonstrates that STEM approaches can yield positive, relevant learning outcomes in aviation safety, especially in PIDS (Voronkin & Lushchin, 2023).

B. Design

The image shows the ESP32-CAM microcontroller integrated with the HC-SR501 PIR sensor. This PIR sensor has three main pins: VCC, output, and ground. The VCC pin, which requires a voltage between 5 and 20V, is connected to the ESP32's 5V pin. The ground pin (GND) is connected to GND on the ESP32, while the output pin is connected to GPIO 12 on the ESP32. The ESP32-CAM microcontroller used is equipped with an onboard connected camera module, so no additional external connections are required for camera operation. This system uses a PIR sensor for motion detection, which triggers the camera to capture an image or perform other actions based on commands programmed into the ESP32. This combination makes the ESP32-CAM with PIR sensor a simple yet effective solution for IoT-based security applications, such as perimeter surveillance.

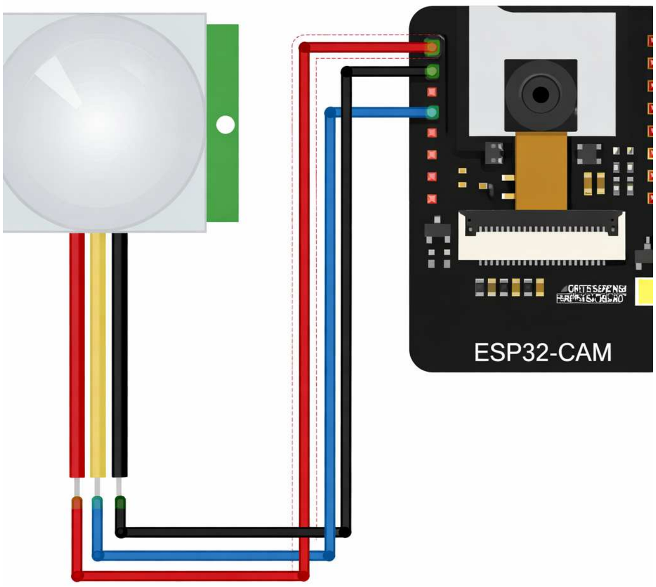

Fig. 2. Design of the tool

C. Design/Coding

1) Install Arduino IDE

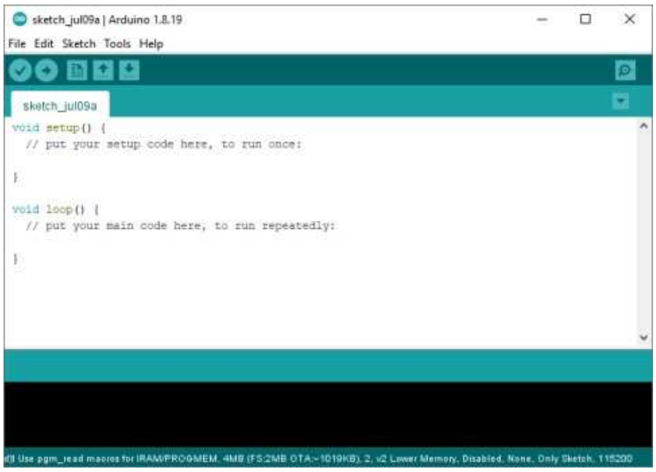

Fig. 3. Arduino IDE Display

The Arduino IDE application used in this study is version 1.8.19. This application can be downloaded from the official Arduino website at [https://www.-arduino.cc/en/software/OldSoftwareReleases](https://www.arduino.cc/en/software/OldSoftwareReleases). During operation, the Arduino IDE requires installing a special library and board for the ESP32. The ESP32 library and board are essential for developing and creating command programs for the ESP32-CAM microcontroller. With the support of the right libraries, the application can be effectively used to program, test, and implement devices based on microcontroller technology, such as the ESP32, including in projects related to the Internet of Things (IoT) and sensor-based security systems, such as the Perimeter Intruder Detection System (PIDS).

2) Install Arduino Blynk

After installing the Arduino IDE and setting up the ESP32 library and board, the researcher proceeded to install Blynk software version 2.27.11. Blynk is used to connect the ESP32-CAM microcontroller to a mobile phone app, enabling real-time control and monitoring of the system. The app plays a key role in the Perimeter Intruder Detection System (PIDS) project, allowing researchers to receive live notifications and monitor movements detected by PIR sensors via mobile devices.

ISSN: 0215-9643
e-ISSN: 2442-8655

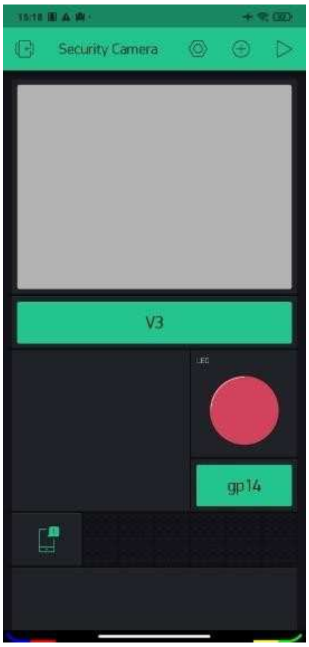

Fig. 4. Blynk Display

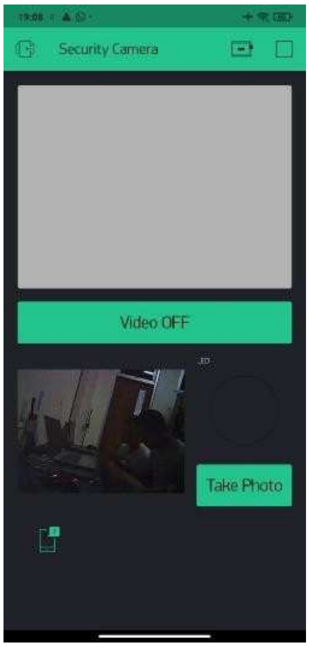

Fig. 5. Blynk connected

The Blynk software version 2.27.11 used in this study is not officially available, but can be downloaded from various Google search results. Since this version is not official, users need to run the command program on a community-developed local server. This local server can be found via various online sources and supports the connection between the ESP32-CAM device and the Blynk application in the Perimeter Intruder Detection System (PIDS) project.

D. Testing

1) Blynk Testing

The connectivity test between the Blynk application and the ESP32 device was performed by connecting the mobile phone to the same Wi-Fi network as the ESP32 device. This step is an important part of testing to ensure that the Blynk application functions optimally for monitoring and controlling the security devices designed. By using the same local network, it is hoped that the connection between the app and the device can run smoothly without interruption. The test results showed that the Blynk app successfully connected to the ESP32 device, indicating that communication between the devices was working. This success ensures that the ESP32 device can receive commands and send real-time notifications through the Blynk app, as planned for the Perimeter Intruder Detection System (PIDS). The image below shows an example of successful connectivity between the app and the ESP32 device, confirming that the system has operated according to the original design and purpose, as shown in Figure 5.

2) Testing Passive Infrared Receiver

The primary purpose of the Passive Infrared (PIR) sensor trial is to detect human movement in the monitored area. PIR sensors detect changes in the infrared radiation emitted by the human body as it moves through the sensor's field of view. During the test, the PIR sensor was connected to the ESP32 module, and the motion detection results were monitored in the Arduino IDE serial monitor. When the PIR sensor detects motion, the value displayed on the monitor's serial port is "1," indicating that motion has been detected. Conversely, if no motion is detected, the value shown is "0," suggesting that the PIR sensor is on standby.

This test was conducted to verify whether the sensor could accurately detect movement within the specified range. The test results showed that the PIR sensor functioned as expected, detected human movement well, and transmitted signals that could be interpreted by an IoT-based security system designed with the ESP32 and the Blynk app. This data provides confidence that the sensor is functioning as intended and is ready for use in a broader security system, such as the Perimeter Intruder Detection System (PIDS) application.

Fig. 6. Uji coba sensor PIR

Researchers tested the accuracy of PIR sensors by detecting human movement at various distances within the room. The test was carried out to determine the extent to which the sensor accurately detects movement. These experiments involve placing human objects at varying distances from the sensors, and each experiment is repeated multiple times to ensure consistent results. The test results show the PIR sensor's effective range and provide important information for improving the perimeter security system under development.

Table 4. Experimental Table I

Distance (m)	Notification	Notification Send Time (seconds)	Response Time Take Photo	Information
1 meter	Sent	1	2,5	Detect motion
2 meters	Sent	2	3	Detect motion
3 meters	Sent	2	2	Detect motion
4 meters	Sent	1	2	Detect motion
5 meters	Sent	2	1	Detect motion
6 meters	Sent	2	3	Detect motion
7 meters	Not Delivered	-	-	Not Detecting
8 meters	Not Delivered	-	-	Does not detect

The first test table shows that the PIR sensor cannot detect movement at a distance of 7 meters, so it does not send a notification to the Blynk application.

Table 5. Experimental Table II

Distance (m)	Notification	Notification Send Time (seconds)	Photo Response Time (seconds)	Information
1 meter	Sent	1	2,5	Detect motion
2 meters	Sent	1	3	Detect motion
3 meters	Sent	2	3	Detect motion
4 meters	Sent	1	2	Detect motion
5 meters	Sent	1	3	Detect motion
6 meters	Sent	2	3	Detect motion
7 meters	Sent	2	2	Detect motion
8 meters	Not delivered	-	-	Does not detect

The second experimental table shows that the PIR sensor can detect movement at a distance of 7 meters, triggering a notification to the Blynk application. At a distance of 8 meters, the PIR sensor cannot detect movement and does not send messages.

Table 6. Experimental Table III

Distance (m)	Notification	Notification Send Time (seconds)	Photo Response Time (seconds)	Information
1 meter	Sent	1	2	Detect motion
2 meters	Sent	2	2	Detect motion
3 meters	Sent	2	2,5	Detect motion
4 meters	Sent	1	2,5	Detect motion
5 meters	Sent	2	3	Detect motion
6 meters	Sent	2	2	Detect motion
7 meters	Not delivered	-	-	Does not detect
8 meters	Not delivered	-	-	Does not detect motion

Based on the test results in Tables 4, 5, and 6, it can be observed that across eight experiments, each run 3 times with human objects, the passive infrared sensor can detect a maximum movement of 7 meters. At distances of 1-6 meters, the PIR sensor reliably detects movement and sends notifications. However, at a distance of 7 meters, the PIR sensor sometimes detects movement and sometimes does not. In 3 experiments on a 7-meter sample, the PIR sensor detected only one event and successfully sent a notification. In the experiment, the PIR sensor failed to detect movement at a distance of 8 meters and did not send messages.

Table 7. Angle Testing

Sudut	Detect
0°	Already
120° Kiri	Already
120° Kanan	Already
135° Kiri	Tidak
135° Kanan	Tidak

The next test aims to measure the PIR sensor's detection angle range for human movement. According to the datasheet, the PIR sensor has a maximum detection angle of 120°. The test results confirm that the sensor operates optimally in detecting movement up to the angle limit. In addition, the PIR sensor's sensitivity can be adjusted to tune detection distance and angle. Increasing sensitivity increases the sensor's detection area, enabling detection at a wider angle. Conversely, a decrease in sensitivity will reduce the detection range, reducing the sensor's ability to detect movement at greater angles and distances.

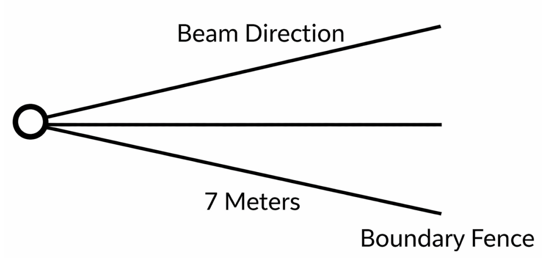

Fig. 7. PIR sensor courtship image

After a series of tests, the device could detect movement up to 7 meters with the appropriate beam coverage, as shown in the previous image.

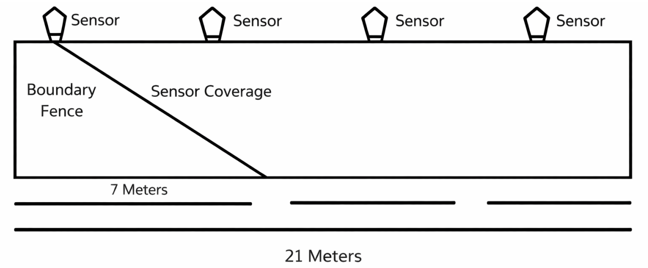

Fig. 8. Side view of tool placement

To overcome the PIR sensor's limitations in distance detection, the device was installed at 7-meter intervals. Based on the simulation shown in the previous image, if the fence reaches a total length of 21 meters, it takes three sensor units to cover the entire area. All of these sensors can be connected to a single microcontroller to simplify the setup and installation of security systems while maintaining efficient monitoring.

3) Camera Module Testing

The test was conducted under two conditions: with the ESP32 module connected to a Wi-Fi network and without it. The results of this test are presented in the table below. In addition, the test includes an evaluation of the camera's functionality to ensure it operates properly in both conditions. This test aims to identify differences in the performance of security systems, especially in connectivity and camera operation, when the ESP32 module is connected to the network.

Table 8. Camera module testing

Wifi	**Camera**	
	Picture	***Video***
Connected	Can Take Picture	Can Display Video
Not Connected	Unable to Taking Photos	Unable to Displaying Videos

E. Tool Validation

It can be seen from the results of filling in the data provided to the validator that the aim is to identify the assessments, criticisms, and suggestions on the product from experts. Lecturers at Surabaya Aviation Polytechnic conducted product validation. The assessed aspects include the software, visual design, and tool functionality, and meet the feasibility indicators for the tool.

Results of filling in the validation data of the tool:

$$eligibility\ \% = \frac{34}{36}\ x\ 100\%$$

$$= \mathbf{94}\%$$

The validation results show that the IoT-based security system with a Placan ESP32-CAM and a camera has a feasibility of 94%, placing it in the "very feasible" category. This assessment covers both technical and functional aspects, with a focus on application in Aviation Security (AVSEC) courses using a STEM approach. The Perimeter Intruder Detection System (PIDS), based on Arduino and PIR sensors, is considered an effective security device for use in educational and field settings.

IV. Conclusion

Based on the study results, the application of the Science, Technology, Engineering, and Mathematics (STEM) approach significantly improves students' conceptual understanding of Perimeter Intruder Detection Systems (PIDS) in the Aviation Security (AVSEC) course. The results of the Paired Sample T-Test showed a significant improvement in students' understanding after participating in STEM-based learning, with an average difference of -17.750 between the pre-test and post-test and a significance level of 0.000. This shows that the STEM approach is practical in deepening students' understanding of aviation security technology. The development of the PIDS system using the Research and Development (R&D) method and the Waterfall approach on hardware and software also provides a more practical and applicable learning experience for students. This research makes a significant contribution to the development of STEM-based learning methods in aviation safety, particularly in PIDS.

References

Achzab, A. M., Putra, A. W., & Yulizar, N. H. (2018). Pengaruh Pembelajaran STEM Terhadap Pemahaman Konseptual dan Kemampuan Teknis Mahasiswa. Jurnal Pendidikan Teknologi, 7(2), 45-53.

Bashir, A., Rehman, K. U., & Gill, N. (2019). Exploring the Role of IoT in Aviation Security: A Case Study of Perimeter Intrusion Detection Systems. International Journal of Aviation Technology, 6(1), 12-19.

Gilder, J., & O'Rourke, M. (2018). Hands-on Learning in STEM Education: Benefits and Challenges. STEM Education Review, 4(2), 88-94.

Görgülü Arı, A., & Meço, Z. (2021). STEM Education Practices and Their Effects on Students' Science, Technology, Engineering, and Mathematics Achievements. Educational Sciences: Theory & Practice, 21(3), 72-85.

Irianto, B., & Novianti, A. (2020). Pemanfaatan Sensor PIR dan Mikrokontroler dalam Sistem Deteksi Intrusi Berbasis IoT. Jurnal Teknologi Informasi dan Komunikasi, 12(3), 104-111.

Johnson, R., Reynolds, M., & Pierson, S. (2022). Teaching STEM with Arduino: Addressing Technological Challenges in Higher Education. Journal of Educational Technology, 8(1), 56-68.

Karoly, L. A. (2017). Enhancing Aviation Security: Strategies and Technologies for Countering Terrorist Threats. RAND Corporation, 2017.

Kelley, T. R., & Knowles, J. G. (2016). A Conceptual Framework for Integrated STEM Education. International Journal of STEM Education, 3(1), 11-23.

Kuo, Y. H., & Wu, Y. H. (2019). Enhancing Airport Perimeter Security with IoT and AI-based Systems. Journal of Aerospace Engineering and Technologies, 5(2), 53-65.

Mpofu, V. (2019). Project-Based Learning: Benefits, Challenges, and Potential in Engineering Education. Journal of Engineering Education, 6(1), 34-45.

Ortiz-Revilla, J., Adúriz-Bravo, A., & Greca, I. M. (2021). Developing 21st Century Skills in STEM Education: A Critical Review of Literature. Science & Education, 30(3), 473-494.

Pressman, R. S. (2015). Software Engineering: A Practitioner's Approach (8th ed.). McGraw-Hill Education.

Rahmawati, D., Sudaryanto, T., & Irawan, F. (2022). Implementasi Internet of Things dalam Pengembangan Sistem Keamanan Perimeter Berbasis Arduino. Jurnal Teknologi Informasi, 9(4), 102-110.

Stewart, M. G., & Mueller, J. (2018). Assessing the Cost-Effectiveness of Aviation Security Measures. Journal of Air Transport Management, 67, 119-125.

Takeuchi, M. A., Cawthon, S., & Turner, E. E. (2020). Interdisciplinary Approaches to STEM Education: Bridging Disciplines, Contexts, and Practices. Journal of STEM Education Research, 3(1), 47-67.

Teixidó, J., Isern, D., & Giné, X. (2021). Smart Detection Systems for Airport Perimeter Security: An IoT Approach. Sensors and Applications in Aviation, 11(5), 789-797.

Voronkin, A., & Lushchin, V. (2023). Project-Based Learning in STEM Education: The Integration of Arduino into University Curriculum. Journal of STEM Integration, 9(1), 102-115.

Wawan, R., Utomo, E., & Siswanto, D. (2022). Integrating STEM and IoT in the Aviation Security Education Curriculum: Enhancing Students' Practical Skills and Conceptual Understanding. International Journal of Aviation Studies, 12(4), 45-59.

.