Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 21 No. 13 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v21i13.57783

PAPER

Design and Educational Application of a Dual-MCU-Based Hardware Kit for IoT Security Practice

Dong-won Kim (✉)

Konyang University, Chungcheongnam-do, Republic of Korea

blast@konyang.ac.kr

ABSTRACT

The proliferation of Internet of Things (IoT) devices has escalated cybersecurity threats, demanding practical, hands-on education for security professionals. However, traditional lecture-based learning and software-only simulations often fail to provide an immersive experience with hardware vulnerabilities. To address this gap, we designed and developed the "Hacker Board," a novel educational hardware kit featuring a dual-MCU architecture that enables simultaneous attack and defense exercises on a single board. The kit is modular, supporting various IoT communication protocols such as IR, RF, RFID, and CAN. We implemented a pedagogical model combining flipped learning with Bloom's Taxonomy and conducted a three-year case study (2022–2024) with undergraduate information security students to evaluate its effectiveness. A mixed-method approach was used, collecting quantitative survey data on student satisfaction, interest, and engagement, alongside qualitative interview data. The findings show consistently high student satisfaction (average 4.47/5.0), interest, and engagement, with scores trending upward over the three years. Qualitative feedback confirmed that the hands-on, hardware-based labs significantly enhanced students' practical skills and learning immersion. This study concludes that the Hacker Board, coupled with a structured pedagogical model, serves as a promising and validated tool for overcoming the limitations of conventional cybersecurity education and provides a replicable framework for hands-on IoT security training.

KEYWORDS

cybersecurity education, Internet of Things (IoT) Security, flipped learning, Bloom's Taxonomy, engineering education, hardware kit, hands-on learning

1 INTRODUCTION

1.1 The rise of IoT and the need for practical security education

The proliferation of Internet of Things (IoT) technology is rapidly advancing our society into a hyper-connected era, where the boundaries between the physical and

Kim, D.-W. (2025). Design and Educational Application of a Dual-MCU-Based Hardware Kit for IoT Security Practice. *International Journal of Online and Biomedical Engineering (iJOE)*, 21(13), pp. 16–30. https://doi.org/10.3991/ijoe.v21i13.57783

Article submitted 2025-08-04. Revision uploaded 2025-09-09. Final acceptance 2025-09-09.

virtual worlds are increasingly blurred [1]. This paradigm shift brings unprecedented innovation, but it also broadens the attack surface for cybersecurity threats, which now have the potential to cause significant real-world damage [2]. Consequently, the growing complexity of these threats presents a substantial challenge to conventional security education [3].

Traditional cybersecurity education, primarily reliant on theoretical lectures, struggles to prepare professionals for the practical challenges of the IoT environment. There is a distinct gap between theoretical knowledge and the skills required to analyze and defend against hardware-level vulnerabilities in embedded systems and IoT devices [4]. In response, the convergence of education and technology, known as EduTech, has gained significant attention as a means to revolutionize learning environments [5]. Specifically for cybersecurity, hardware-based educational tools are essential for providing a tangible training ground that software simulations alone cannot replicate [4].

1.2 Limitations of existing educational approaches (Research gap)

Despite the clear need for practical training, conventional cybersecurity education remains heavily reliant on lecture-based learning, which is often insufficient for developing the deep problem-solving skills required in the field [6]. To bridge this gap, online platforms and software-based simulations have emerged, but they cannot adequately replicate the physical-layer vulnerabilities found in IoT devices and embedded systems [4]. The security of these systems often depends on hardware-specific interactions, which are impossible to simulate fully in a virtual environment.

This leaves a critical void in the training of security professionals. Consequently, there is a clear research gap for a comprehensive educational solution that combines both hardware and pedagogy. A need exists for a dedicated, integrated hardware platform that allows students to experience tangible attack and defense scenarios [4]. Furthermore, the mere existence of a tool is not enough; its effectiveness hinges on its integration into a structured pedagogical framework designed to maximize learning outcomes, which itself requires empirical validation [7, 8]. This study directly addresses this gap by presenting not only the design of such a hardware kit but also the empirical validation of its application within a specific instructional model [4, 7].

To guide this study, we formulated the following research questions:

- (RQ1) How can a dedicated hardware kit be designed to effectively facilitate integrated, hands-on IoT security attack and defense exercises in an educational setting?
- (RQ2) What is the impact of integrating this hardware kit into a pedagogical model combining flipped learning and Bloom's Taxonomy on undergraduate students' learning satisfaction, interest, and practical skill development?

1.3 Research objectives and contributions

To address the research gap identified above, this paper has two primary objectives. The first objective is to present the comprehensive design and architecture of the "Hacker Board," a novel educational hardware kit specifically developed for hands-on IoT security training [4]. We detail its core features, including the

dual-MCU structure for integrated attack-defense exercises and the modular design that supports a wide range of security scenarios. The second objective is to introduce and empirically validate a pedagogical model that leverages this hardware for effective learning [7]. This involves the application of a flipped learning framework combined with Bloom's Taxonomy, evaluated through a three-year case study with undergraduates.

This study makes the following contributions to the field of cybersecurity and engineering education: First, it provides a tangible and replicable hardware solution that overcomes the limitations of software-only simulations and general-purpose development boards [4]. Second, it offers empirical evidence demonstrating that the integration of a dedicated hardware tool with a structured, hands-on pedagogical model significantly enhances student engagement, practical skills, and interest in cybersecurity [7]. Collectively, this study presents a complete and validated framework from hardware design to pedagogical application and effectiveness analysis for developing the next generation of practically skilled cybersecurity professionals.

This study integrates and expands upon two prior works by the author. The technical design and specifications of the 'Hacker Board,' a hardware kit for IoT security education, were detailed in a previous study. A separate study was also conducted to develop a pedagogical model combining flipped learning and Bloom's Taxonomy, and its effectiveness was empirically analyzed over a three-year period. The current paper synthesizes these two streams of research to systematically present the entire process, from the educational rationale behind the hardware design to the application of the pedagogical model and its long-term validation. In doing so, it provides a comprehensive framework for an international academic audience and clarifies its unique contribution through a comparative analysis with alternative educational platforms.

2 RELATED WORKS

To situate this study within the existing academic landscape, this chapter reviews the relevant literature in two key areas. First, it examines the hardware platforms currently utilized in cybersecurity education, analyzing their strengths and identifying their limitations in addressing the specific needs of IoT security training. Second, it explores established pedagogical models for hands-on learning in engineering, providing the theoretical foundation for the instructional framework developed in this research. This review collectively serves to further establish the context and justify the research gap that the "Hacker Board" and its associated teaching model are designed to fill.

2.1 Hardware platforms for cybersecurity education

The use of physical hardware is widely recognized as a method to enhance hands-on learning in computer science and engineering education [9]. In this context, general-purpose platforms such as Arduino and Raspberry Pi have gained significant popularity [5]. Their low cost, extensive community support, and flexibility make them accessible tools for a variety of educational projects. However, when applied to the specialized field of cybersecurity, these platforms exhibit notable limitations. They are not inherently designed for security education, requiring instructors to

expend considerable effort to develop and configure separate systems for demonstrating attack and defense scenarios [4]. This often results in a fragmented learning experience and a steep setup curve for both educators and students [10].

This highlights the need for specialized educational hardware designed from the ground up for cybersecurity [11]. An ideal platform should provide an integrated, all-in-one environment that simplifies the complex process of setting up security labs [12]. Key features should include built-in capabilities for both attacking and defending a target, modular support for various IoT communication protocols, and a structured curriculum with pre-designed hacking scenarios [4]. The absence of such a comprehensive and user-friendly tool in the market constitutes a significant barrier to effective, hands-on IoT security education, as summarized in Table 1.

Table 1. A comparative analysis of educational hardware platforms for cybersecurity education

Feature	Hacker Board	General-Purpose Platforms (e.g., Raspberry Pi, Arduino)
Primary Purpose	Dedicated to hands-on IoT security education, allowing for the simulation of real-world hacking and defense scenarios.	Designed for general-purpose programming, electronics, and a wide range of IoT projects, not specifically for security.
Core Architecture	Features an integrated Dual-MCU system on a single board, enabling simultaneous "Attacker" and "Defender" exercises.	Built on a single processor, requiring two separate devices and complex networking to simulate an attack and defense environment.
Hardware Usability	Utilizes magnetic, "plug-and-play" modules, which simplifies setup and allows for rapid changes between different lab scenarios without manual wiring.	Requires manual wiring with breadboards and jumper cables, which can be time-consuming and prone to errors for beginners.
Curriculum Support	Provides a structured, scenario-based curriculum, including a textbook and source code, specifically designed for a 15-week cybersecurity course.	Lacks a dedicated, built-in curriculum for security; educational content must be independently developed by the instructor or sourced from disparate community projects.

2.2 Pedagogical models for hands-on learning in engineering

The effectiveness of any educational tool is fundamentally linked to the pedagogical model through which it is implemented. Simply providing hardware is insufficient; a structured teaching framework is necessary to guide student learning and maximize engagement [6].

One prominent model is flipped learning, which inverts the traditional classroom by having students engage with theoretical content before class, reserving in-class time for hands-on, problem-solving activities [8]. This approach fosters active learning and has been shown to be effective in various contexts [13]. However, its application to complex hardware labs requires a carefully structured progression of activities to prevent student frustration and ensure foundational concepts are mastered [14].

To provide this structure, Bloom's Taxonomy offers a valuable framework. It classifies cognitive skills into a hierarchy, from lower-order skills such as 'Remembering' and 'Understanding' to higher-order skills such as 'Analyzing,' 'Evaluating,'

and 'Creating' [15]. By designing learning activities that guide students progressively up this hierarchy, educators can build a logical and effective learning path [16]. This study posits that the synergy between flipped learning and Bloom's Taxonomy creates an optimal model for hardware-based cybersecurity education (see Figure 1). Flipped learning provides the macro-structure for organizing learning, while Bloom's Taxonomy provides the micro-structure for designing the hands-on activities themselves, guiding students from basic understanding to creative problem-solving [7].

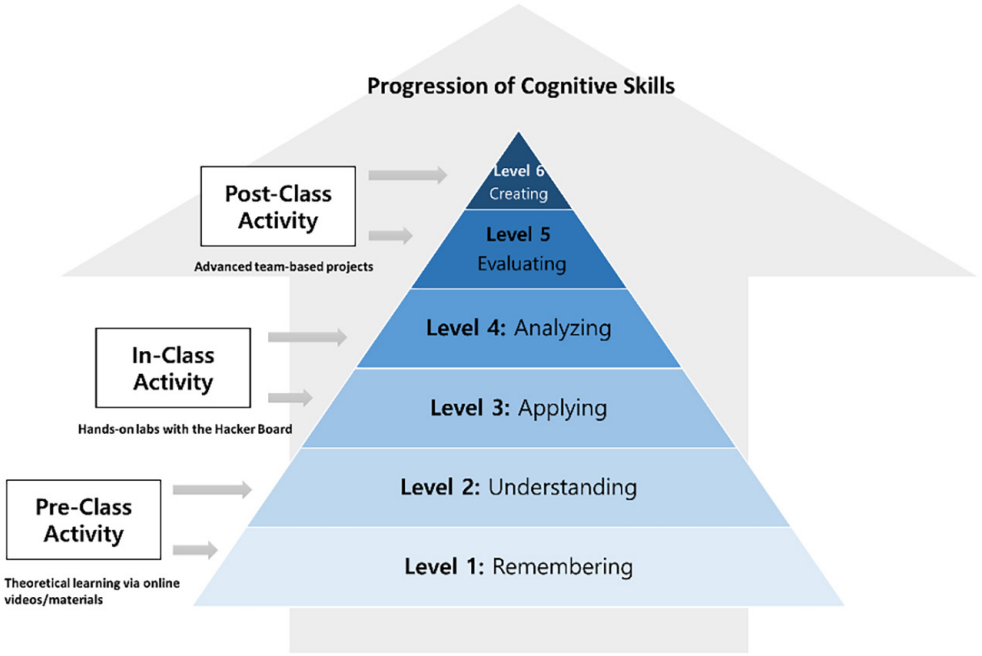

Fig. 1. The integrated pedagogical model combining flipped learning and Bloom's Taxonomy

3 DESIGN OF THE HACKER BOARD HARDWARE KIT

This chapter details the design and architecture of the "Hacker Board," the novel hardware kit developed to address the limitations of existing educational platforms discussed in Chapter 2. We begin by outlining the core pedagogical and practical strategies that guided the entire design process. Subsequently, we present the overall system architecture, focusing on its central feature, the dual-MCU system for integrated attack-defense simulation. Finally, we describe the flexible, modular design of the sensor and communication components, which allows the kit to be adapted for a wide range of IoT security topics.

3.1 Core design strategies

The development of the Hacker Board was not arbitrary; it was guided by a set of eight core strategies (S1–S8) intended to maximize its educational effectiveness, usability, and flexibility (refer to Table 2). These principles ensured the final product would be more than just a collection of components but a cohesive educational tool. Key strategies included designing for easy maintenance and repair (S1), enabling rapid assembly and disassembly to make efficient use of limited class

time (S2), and ensuring expandability for future technologies through a modular structure (S3). Most importantly, a core strategic goal was to facilitate the convenient simulation of both attack and defense scenarios on a single, integrated board (S6), a feature absent in general-purpose platforms [4].

Table 2. Core design strategies (S1–S8) for the Hacker Board

Strategy ID	Hacker Board	
S1	**Maintainability**	Designed for easy replacement of parts, simple inventory management, and quick repairs to ensure longevity and low upkeep costs
S2	**Efficiency**	Enables rapid assembly and disassembly of modules to maximize the use of limited class time for programming and hands-on activities.
S3	**Expandability**	Ensures ease of improvement and updates through a modular sensor system, allowing for future customization and the addition of new technologies.
S4	**Open Source**	Utilizes open-source hardware and software principles to ensure easy access, encourage modification, and foster a collaborative community.
S5	**Programmability**	Provides a convenient and familiar programming environment by leveraging widely used platforms (e.g., Arduino IDE).
S6	**Functional Simulation**	Facilitates the convenient simulation of both attack and defense functions on a single board, simplifying the setup of complex security scenarios.
S7	**Portability**	Designed for easy transport, enabling use in various settings from formal classrooms to remote or home-based learning environments.
S8	**Cost-Effectiveness**	Aims to provide a powerful educational tool at a competitive and affordable price point.

The Hacker Board is a purpose-built educational kit designed to overcome the limitations of traditional, software-based cybersecurity education. Its core architecture is based on a dual Microcontroller Unit (MCU) system within a single board, featuring two ATmega328P MCUs, which are the processors used in the popular open-source Arduino Uno. This dual-MCU design is the Hacker Board's most distinctive feature, enabling simultaneous and independent execution of attack (attacker) and defense (defender) simulations. This allows students to observe the direct cause and effect of cybersecurity exploits and countermeasures in real time. The board is designed modularly, with a variety of sensor and communication modules that can be easily attached or detached via magnetic connectors, minimizing setup time and maximizing durability in a classroom setting.

3.2 System architecture and components

The central innovation of the Hacker Board's architecture is its dual-MCU system, which is illustrated in the diagram (see Figure 2). The board incorporates two independent ATmega328P microcontrollers, the same MCU that powers the ubiquitous

Arduino platform. This choice of MCU ensures accessibility and a familiar programming environment for a wide range of students and educators [4].

One MCU is designated as the "Attacker" and the other as the "Defender," with each being independently programmable. This unique structure allows a single board to emulate a complete cybersecurity scenario, where one part of the system actively attacks the other. The two MCUs are interconnected, typically via a UART serial interface, allowing them to exchange data and simulate the communication channel between a hacker and a target system. The mainboard also integrates essential supporting components, including a stable power supply system (24V to 5V DC-DC converter), USB hubs for connectivity, and standardized ports for attaching the various functional modules [4].

The design of the Hacker Board was guided by several key principles to maximize its educational effectiveness and accessibility.

- Open-Source Foundation: By utilizing the ATmega328P MCU and compatibility with the Arduino IDE, the Hacker Board is rooted in a robust, open-source ecosystem. This allows instructors and students to leverage a vast amount of existing documentation, libraries, and community support, lowering the barrier to entry and enabling customization.
- Cost-Effectiveness: While a precise bill of materials is beyond the scope of this paper, the board's cost-effectiveness stems from its all-in-one design. It integrates functionalities that would otherwise require purchasing numerous separate Arduino shields, sensors, and breakout boards for protocols like CAN, RF, and RFID. This integrated approach significantly reduces the total cost and complexity of setting up a comprehensive IoT security lab.
- Curriculum-Aligned Module Selection: The sensor and communication modules were not chosen arbitrarily. They were specifically selected to cover the most common and critical attack vectors in modern IoT ecosystems, including consumer devices (IR, Bluetooth), industrial control systems (Modbus, UART), and automotive networks (CAN). This ensures that the practical exercises directly align with the curriculum's goal of providing wide-ranging, real-world security skills.

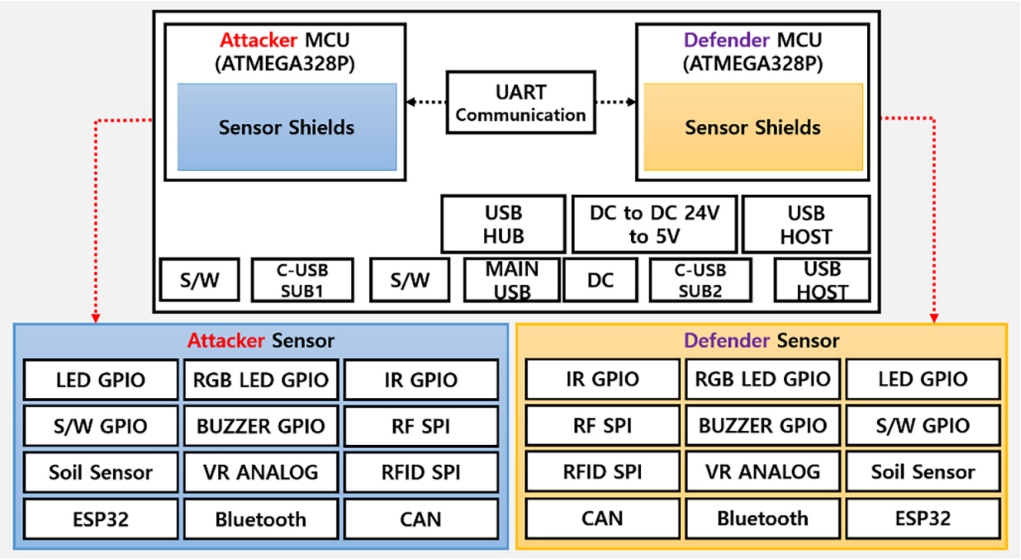

Fig. 2. System architecture of the Hacker Board

3.3 Modular design for flexibility

To ensure flexibility and pedagogical versatility, the Hacker Board was designed with a highly modular structure. Instead of a fixed set of onboard peripherals, various IoT communication interfaces and sensors are implemented as individual, detachable modules. This design allows instructors and students to customize the board for specific learning objectives by simply swapping modules [4].

The supported modules cover a wide curriculum of modern security topics, including infrared (IR), radio frequency (RF), radio-frequency identification (RFID), Bluetooth (B/T), universal asynchronous receiver-transmitter (UART), controller area network (CAN), and Modbus protocols. A key usability feature is the implementation of magnetic connectors for these modules. This "plug-and-play" approach minimizes setup time, prevents connection errors, and enhances the durability of the kit by reducing physical wear from frequent use. This modularity empowers the Hacker Board to serve as a versatile tool, capable of demonstrating everything from simple signal sniffing to complex automotive network hacking within a single, cohesive educational ecosystem [4, 7].

4 CASE STUDY: METHODOLOGY FOR EDUCATIONAL APPLICATION

This section presents the methodology used to empirically evaluate the educational effectiveness of the Hacker Board. To move beyond a purely technical description of the hardware, we conducted a three-year case study within an actual university course. This section first details the integrated instructional model, which combines flipped learning with Bloom's Taxonomy [7]. Next, it describes the participants and the specific educational setting in which the study was conducted [7]. Finally, it explains the mixed-method approach used for data collection and analysis, which combines quantitative survey data with qualitative feedback to provide a holistic assessment of the learning experience [17].

4.1 Instructional model and procedure

The pedagogical approach for this study was designed to maximize active, hands-on learning by integrating the Hacker Board into a structured instructional framework. We adopted a model that synergistically combines flipped learning and Bloom's Taxonomy [7]. The flipped learning model provides the overall structure for the course, dividing the learning process into three phases: 1) pre-class theoretical learning, 2) in-class practical application, and 3) post-class advanced tasks [8].

This structure was further refined by applying the cognitive levels of Bloom's Taxonomy to guide the activities within each phase [15]. The 15-week course was designed to progressively move students from lower-order thinking skills to higher-order ones. The 15-week course was designed to progressively move students from lower-order thinking skills to higher-order ones, as detailed in Table 3.

Table 3. The 15-week curriculum roadmap

Week	Learning Content	Bloom's Stage	Pre-Class (Theory)	In-Class (Practice)	Post-Class (Advanced)
1	IoT Security Overview	Remember	Study IoT concepts and security threats	Discuss IoT threat analysis cases	Explore security problem solutions
2	Hacker Board & Environment Setup	Understand	Learn Hacker Board overview and components	Install drivers and configure environment	Troubleshoot environment setup issues
3	Basic Module Practice 1	Apply	Learn basic electronic circuit principles	Practice with LED and LCD modules	Debug and improve module code
4	Basic Module Practice 2	Apply	Study advanced Hacker Board functions	Practice with Buzzer and Sensor modules	Debug and improve module code
5	IrDA Security & Hacking	Analyze	Study IR security theory and attack cases	Practice IR Sniffing & Attack	Explore security enhancement techniques
6	UART Security & Hacking	Analyze, Apply	Learn serial communication & security concepts	Practice UART Sniffing & Injection	Explore security enhancement techniques
7	RF Security & Hacking	Analyze, Apply	Study RF communication concepts	Practice RF Sniffing & signal modulation	Research RF attack detection strategies
8	Mid-term Theory Exam	Evaluate	Review all theoretical concepts	Take mid-term theory exam	–
9	RFID Security & Hacking	Analyze, Apply	Analyze RFID technology & vulnerabilities	Practice RFID Cloning	Research security response strategies
10	Bluetooth Security & Hacking	Analyze, Apply	Learn Bluetooth protocol concepts	Practice BLE transmission/ reception attacks	Research Bluetooth attack cases
11	Home Router Security & Hacking	Analyze, Apply	Learn home router security concepts	Practice home router hacking	Research security cases & improvement strategies
12	HID Keylogger	Analyze, Apply	Study keylogging concepts and cases	Practice implementing an HID keylogger	Analyze logs and research security enhancements
13	Modbus Security & Hacking	Analyze, Apply	Learn Fieldbus protocol concepts	Practice Modbus attack & defense	Research control system security measures
14	CAN Security & Hacking	Analyze, Apply	Study automotive security cases	Practice CAN Sniffing & Injection	Research CAN defense strategies
15	Final Team Project	Create	Review IoT hacking project background	Present project and share results	Receive final feedback and reflect

The process began with foundational knowledge acquisition (Remembering/ Understanding) in the pre-class phase, moved to hands-on application and analysis of security vulnerabilities using the Hacker Board (Applying/Analyzing) during in-class labs, and culminated in team-based projects where students had to creatively solve complex security challenges and evaluate their solutions (Evaluating/Creating) [7]. This systematic procedure ensured that students built a solid conceptual foundation before tackling complex practical problems.

4.2 Participants and setting

The case study was conducted over three academic years, from 2022 to 2024, at Konyang University. The participants were third-year undergraduate students

majoring in Information Security who were enrolled in the "IoT Security Practice" course. Approximately 100 students participated over the three-year period. This specific cohort was chosen because they possessed foundational knowledge in cybersecurity but lacked significant hands-on experience with hardware-level security, making them an ideal group to assess the impact of the Hacker Board and the associated pedagogical model. The course was a semester-long (15 weeks) elective, providing a consistent and controlled setting for the longitudinal study [7].

4.3 Data collection and analysis

To ensure a comprehensive evaluation, we employed a mixed-method research approach, which combines quantitative and qualitative data to provide a richer understanding of the educational outcomes [17].

Quantitative data was collected through anonymous surveys administered at the end of each semester. These surveys used a 5-point Likert scale to measure students' satisfaction with the course content and teaching method, their level of interest in new technologies, and their perception of how the course contributed to their career preparation and practical skills. Qualitative data was gathered through multiple sources, including student team project reports, direct observation by the instructor during lab sessions, and semi-structured interviews with students. The combined data were analyzed to identify trends in student perceptions over the three years and to understand the specific factors that contributed to the learning outcomes [7].

The author was assisted by an AI writing tool (Google's Gemini) for structuring, paraphrasing, and refining the language of this manuscript based on the author's original research and directives. The author reviewed and takes full responsibility for the final content of this article.

5 RESULTS

This section presents the results of the three-year case study, which evaluated the educational effectiveness of the Hacker Board and its integrated pedagogical model. The findings are presented in two parts. First, we provide a quantitative analysis of student feedback collected through end-of-semester surveys. This is followed by a qualitative analysis of the learning experience, drawing from student reports and interviews to provide deeper context to the numerical data.

5.1 Quantitative analysis of student feedback

Over the three-year period from 2022 to 2024, quantitative data consistently indicated a high level of student satisfaction and engagement with the course. The survey measured three key areas on a 5-point Likert scale: satisfaction with the course, interest in new technologies, and perceived contribution to practical skills and career preparation.

As shown in Figure 3, the average scores across all categories were consistently high, remaining above 4.0 throughout the study period. Notably, there was a steady upward trend in all metrics over the three years. For instance, the average

satisfaction with the educational curriculum increased from 4.3 in 2022 to 4.6 in 2024, demonstrating a progressively positive reception of the hands-on learning experience. While an Analysis of Variance (ANOVA) did not show a statistically significant difference between the years ($p > 0.05$), which may be attributed to the relatively small sample size, the positive trend suggests a sustained and growing educational impact [7].

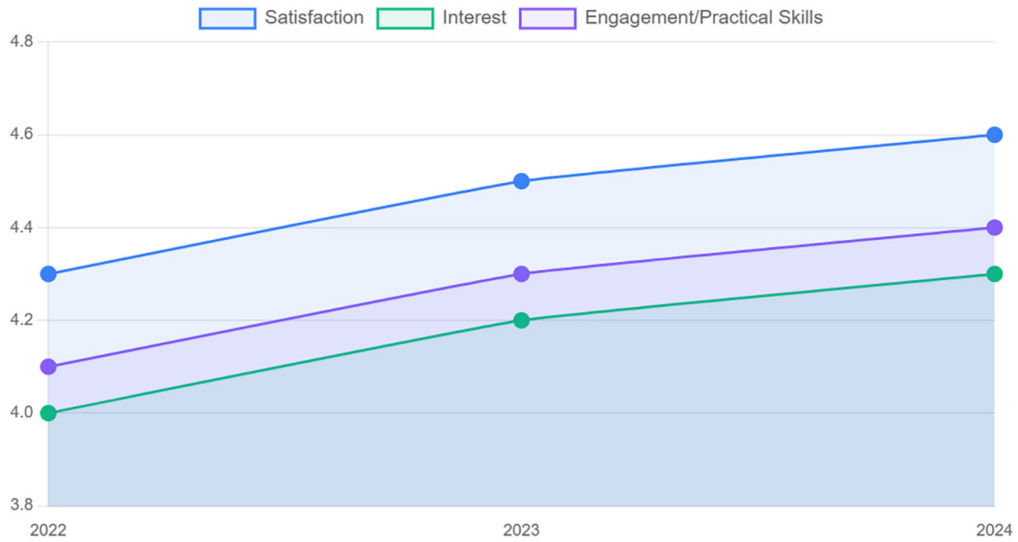

Fig. 3. Trend of student survey results (2022–2024), measuring satisfaction, interest, and engagement/practical skills on a 5-point Likert scale

5.2 Qualitative analysis of learning experience

The qualitative data provided rich, contextual insights that complement the quantitative results. Analysis of student project reports and interview transcripts revealed several key themes.

First, students overwhelmingly reported that the hands-on labs with the Hacker Board significantly improved their understanding of abstract cybersecurity concepts. One student noted, "The theory of signal sniffing was just text in a book until I actually captured and analyzed a real signal with the board. It finally clicked." This sentiment was echoed across multiple participants, who felt that the tangible interaction with hardware was crucial for bridging the gap between theory and practice.

Second, the dual-MCU architecture was frequently cited as a major strength. Students found the ability to program both the "Attacker" and "Defender" on a single device to be highly effective for understanding the dynamics of a cyber-attack. This integrated experience allowed them to see the immediate cause-and-effect relationship between an exploit and its defense, a perspective difficult to gain from separate systems.

Finally, the team-based final projects, which required students to creatively solve a novel security problem, were highlighted as a capstone experience that boosted their confidence and problem-solving skills. This aligns with the higher-order cognitive skills of 'Evaluating' and 'Creating' in Bloom's Taxonomy, suggesting the pedagogical model was successful in guiding students toward advanced learning outcomes [7, 15].

6 DISCUSSION

This section interprets the findings presented in Section 5, contextualizing them within the broader field of cybersecurity education. We first discuss the meaning and significance of the quantitative and qualitative results. We then explore the practical and theoretical implications of this study for educators and curriculum designers. Finally, we transparently acknowledge the limitations of this research and propose specific directions for future work.

To contextualize the contribution of the Hacker Board, Table 4 provides a comparative analysis against general-purpose platforms such as Arduino and Raspberry Pi for the specific task of IoT security training. While platforms such as Arduino and Raspberry Pi offer great flexibility, they require significant setup, additional shields or HATs, and complex wiring to replicate the functionalities integrated into the Hacker Board. The key innovation of the Hacker Board is its dual-MCU architecture, which uniquely enables simultaneous attack and defense exercises on a single device, and its curated set of modules specifically targeting prevalent IoT security vulnerabilities. This all-in-one, purpose-built design lowers the barrier to entry for both instructors and students, making complex IoT security concepts more accessible and cost-effective to implement in an educational setting.

Table 4. Comparative analysis of educational platforms for IoT security training

Feature	Hacker Board	Arduino Uno	Raspberry Pi
Primary Goal	**IoT Security Education**	General-Purpose Prototyping	General-Purpose Computing
Setup Complexity	**Low (All-in-one)**	Medium (Wiring & Shields)	High (OS & Software)
Simultaneous Attack/Defense	**Yes (Integrated Dual MCU)**	No (Single MCU)	No (Single-Board Computer)
Included Peripherals	**High (Built-in IoT modules)**	Low (Requires many add-ons)	Low (Requires add-ons)
Focus on Security Concepts	**High (Purpose-built)**	Low (General purpose)	Low (General purpose)
Cost for Full Lab Setup	**Moderate**	High (Cumulative cost)	High (Cumulative cost)

6.1 Interpretation of findings

The consistently high scores in student satisfaction, interest, and perceived skill development suggest that the educational model built around the Hacker Board was highly successful. The qualitative findings provide a clear explanation for this success: the hardware-based, hands-on approach effectively bridged the gap between abstract theory and practical application [18, 19]. Students' comments about concepts "finally clicking" indicate that the act of physically manipulating hardware and observing real-time results was critical for deep learning. This supports the pedagogical principle that active, problem-based learning is more effective than passive, lecture-based instruction, particularly in technical fields [6, 20].

The upward trend in scores over the three years, while not statistically significant in the ANOVA test, likely reflects the iterative refinement of the course curriculum

and the instructor's growing familiarity with the platform. The non-significant p-value is a probable consequence of the limited sample size; however, the strength of the mixed-method approach [17] allows the rich qualitative data to strongly support the conclusion of the model's effectiveness, a finding consistent with other studies on hands-on cybersecurity labs [21, 22]. The synergy between the specialized hardware [4] and the structured pedagogy [7, 8, 15] appears to be the key factor, creating an environment where students were not only engaged but also systematically guided toward advanced cognitive skills.

6.2 Implications for cybersecurity education

The results of this study offer several important implications. For practitioners and educators, this research provides a validated, replicable framework for implementing hands-on IoT security labs. The Hacker Board itself presents a tangible solution to the limitations of general-purpose hardware, offering an all-in-one platform that reduces setup complexity and is specifically tailored for attack-defense scenarios. The detailed 15-week curriculum model, provided in Table 3, can serve as a practical guide for other institutions seeking to develop similar courses.

Theoretically, this study contributes to the literature by providing empirical evidence for the effectiveness of combining a bespoke hardware tool with the flipped learning and Bloom's Taxonomy models. It demonstrates that the value of an educational tool is maximized when it is embedded within a sound pedagogical structure. This reinforces the idea that innovation in EduTech is not just about creating new technology but about thoughtfully integrating it into the learning process.

6.3 Limitations and future work

Despite the positive findings, this study has several limitations that must be acknowledged. First, the study was conducted at a single university with a specific demographic of undergraduate students. Therefore, the findings may not be directly generalizable to other educational contexts, such as high schools or corporate training programs. Second, as previously noted, the sample size was relatively small, which constrained the statistical power of the analysis. Third, while not frequently reported by students, the intensive, project-based nature of the course could potentially lead to a higher cognitive load for some learners.

These limitations point toward clear directions for future research. A larger, multi-institutional study is needed to validate these findings across different populations and to test for statistical significance with greater power. Future work could also involve a direct comparative study, quantitatively measuring the learning outcomes of the Hacker Board model against a traditional lab using general-purpose hardware. Furthermore, the modular nature of the Hacker Board platform invites the development and testing of new modules that address emerging security threats, such as those related to artificial intelligence, drones, or other specialized IoT ecosystems.

7 CONCLUSION

This study was motivated by the critical gap between traditional, theory-based cybersecurity education and the practical skills required to address real-world IoT

hardware security challenges. To bridge this gap, we designed, developed, and evaluated a comprehensive educational framework centered on a novel hardware platform, the "Hacker Board." The board's unique dual-MCU architecture and modular design provide an integrated, hands-on environment for simulating tangible attack and defense scenarios, which are often overlooked in conventional learning.

Through a three-year case study, we implemented this hardware within a structured pedagogical model that combined flipped learning with Bloom's Taxonomy. The mixed-method evaluation, incorporating both quantitative survey data and qualitative student feedback, demonstrated the effectiveness of our approach. The findings consistently showed high levels of student satisfaction and engagement. More importantly, the qualitative results confirmed that the hands-on interaction with the Hacker Board was instrumental in helping students translate abstract security concepts into practical, applicable skills.

In conclusion, this study contributes a comprehensive and empirically evaluated framework from hardware design to pedagogical implementation and effectiveness analysis for hands-on IoT security education. It offers a replicable model for other educational institutions seeking to move beyond conventional teaching methods and better prepare students for the practical demands of the cybersecurity field. As technology continues to evolve, the development and integration of such innovative, practice-oriented educational solutions will remain crucial in cultivating the next generation of highly skilled security professionals.

8 ACKNOWLEDGMENTS

This paper was supported by the Konyang University Research Fund in 2025.

9 REFERENCES

[1] World Economic Forum, "Annual Meeting of the Global Future Councils 2023," 2023. [Online]. Available: https://www.weforum.org/meetings/annual-meeting-of-the-global-future-councils-2023

[2] J. E. Kim, "An analysis of the effect of artificial intelligence on human society," *The Journal of the Convergence on Culture Technology (JCCT)*, vol. 5, no. 2, pp. 177–182, 2019.

[3] H. Yoon, "A study on Edu-Tech activation methods for learners in university education," *The Journal of Humanities and Social Science*, vol. 13, no. 1, pp. 3135–3148, 2022. https://doi.org/10.22143/HSS21.13.1.222

[4] D.-W. Kim, "Design of hardware (Hacker Board) for IoT security education utilizing dual MCUs," *Journal of Convergence Security*, vol. 24, no. 1, pp. 43–49, 2024. https://doi.org/10.33778/kcsa.2024.24.1.043

[5] B. Seo, "EduTech, and 'A place called school'," in *Proc. Korean Society for the Study of Sociology of Education*, 2021, pp. 59–82.

[6] S. V. Devika, A. Siddapuram, R. Kaur, and A. Bollampally, "From lecture-based learning to problem-based learning: A review on navigating the transformation in engineering education," *Journal of Engineering Education & Technology*, vol. 38, pp. 179–183, 2024. https://journaleet.in/index.php/jeet/article/view/2272

[7] D.-W. Kim, "Development and empirical study of a hardware (Hacker Board)-based cybersecurity instructional model," *Journal of Convergence Security*, vol. 25, no. 1, pp. 123–132, 2025. https://doi.org/10.33778/kcsa.2025.25.1.123

[8] J. Bergmann and A. Sams, *Flip Your Classroom: Reach Every Student in Every Class Every Day*. Washington, DC: Internal Society for Technology in Education, 2012.
[9] C. Torres-Perez *et al.*, "Influence of higher education on IoT acceptance through hands-on learning," *TEM Journal*, vol. 14, no. 1, pp. 528–539, 2025. https://doi.org/10.18421/TEM141-47
[10] X. Fu *et al.*, "Building a low-cost and state-of-the-art IoT security hands-on laboratory," in *Proc. of the 51st ACM Technical Symposium on Computer Science Education*, 2020, pp. 101–107.
[11] P. Patras, "IoT education kit compiled by Paul Patras now available via Arm University program," University of Edinburgh News, 2021.
[12] A. Al-Darwesh *et al.*, "Optimizing cybersecurity education: A comparative study of on-premises and cloud-based lab environments using AWS EC2," *Journal of Cybersecurity and Privacy*, vol. 4, no. 8, p. 297, 2024. https://doi.org/10.3390/computers14080297
[13] S. H. Kim and J. Huh, "A systematic review of flipped learning research in domestic engineering education," *Journal of Engineering Education Research*, vol. 24, no. 3, pp. 24–34, 2021.
[14] G. B. Folayan and A. Ibrahim, "Applying project based learning to flipped bloom taxonomy for deep understanding in control systems," *International Journal of Engineering Research & Technology*, vol. 14, no. 8, 2025.
[15] B. S. Bloom, *Taxonomy of Educational Objectives: The Classification of Educational Goals*. New York, NY: Longmans, Green, 1956.
[16] R. Kwan *et al.*, "Reimagining flipped learning via Bloom's Taxonomy and Student–Teacher–GenAI interactions," *Education Sciences*, vol. 15, no. 4, p. 465, 2025. https://doi.org/10.3390/educsci15040465
[17] J. W. Creswell and V. L. Plano Clark, *Designing and Conducting Mixed Methods Research* 3rd ed. Thousand Oaks, CA: SAGE Publications, 2017.
[18] Cybrary, "Hands-on cybersecurity training: Why practical labs are essential," Cybrary Blog, 2025.
[19] INE, "Hands-on labs: The key to effective cybersecurity education," INE Blog, 2024.
[20] P. Vajpayee *et al.*, "Enhancing cybersecurity education through project-based learning," in *Proc. of the 2025 ASEE Annual Conference & Exposition*, 2025.
[21] S. T. Ahmed *et al.*, "Remote labs in cybersecurity education: A comprehensive analysis," *ACM Transactions on Computing Education*, vol. 25, no. 3, 2025.
[22] S. B. Obukhov, V. A. Kireev, I. V. Korytin, N. V. Evseeva, and E. V. Romanova, "Developing an IoT-based engaged student learning environment and tools for engineering and computer science," in *Proc. of the 2023 ASEE Annual Conference & Exposition*, 2023.

10 AUTHOR

Dong-won Kim is an Associate Professor in the Department of Smart Security at Konyang University. He received his Ph.D. in Information Security from the Graduate School of Information Security at Korea University. His research interests include convergence security, IoT security, and AI security (E-mail: blast@konyang.ac.kr).