International Journal of Advanced Technology and Engineering Exploration, Vol 11(121)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2024.111101097

Research Article

Enhancing cybersecurity awareness through mobile learning: a study on vocational accounting and finance students

Fivia Eliza[1], Radinal Fadli[2*], Yayuk Hidayah[3], Herman Dwi Surjono[4] and Ratna Candra Sari[5]
Faculty of Engineering, Universitas Negeri Padang, Padang, Indonesia[1]
Faculty of Information Technology Education, Universitas Muhammadiyah Muara Bungo, Bungo, Indonesia[2]
Faculty of Social Sciences, Law and Political Sciences, Yogyakarta State University, Yogyakarta, Indonesia[3]
Faculty of Engineering, Yogyakarta State University, Yogyakarta, Indonesia[4]
Faculty of Economics and Business, Yogyakarta State University, Yogyakarta, Indonesia[5]

Received: 25-June-2024; Revised: 12-December-2024; Accepted: 16-December-2024

Abstract
The rapid growth of the digital economy poses significant cybersecurity threats, particularly for individuals in accounting and finance. This study investigates the effectiveness of a mobile-based learning program in enhancing cybersecurity awareness among accounting and finance students. The research employs a 4D model approach (Define, Design, Develop, Disseminate). The instruments used include validity and reliability questionnaires, cybersecurity awareness tests, and effectiveness surveys. The mobile learning-based cybersecurity program developed was validated through expert assessment. Test results revealed a significant improvement in cybersecurity awareness among accounting and finance students. The key advantages of this approach include increased student engagement, high accessibility, lower costs, and applicability for students without a technology background. This study provides empirical evidence supporting the enhancement of students' cybersecurity understanding, enabling them to be more vigilant and proactive in safeguarding financial information. These findings can also inform policy development regarding the integration of cybersecurity education into institutional curricula. Given the success of mobile learning programs, further research is recommended to explore their long-term impacts and to customize learning content for diverse fields of expertise.

Keywords
Cybersecurity awareness, Mobile learning, Accounting and finance education, Digital economy threats, Educational technology.

1.Introduction
The digital revolution has ushered in a new era of connectivity and innovation, transforming the way we live, work, and manage our finances. However, like a double-edged sword, these advancements have also paved the way for increasingly dangerous cyber threats [1]. In Indonesia, where digital transactions have surged in recent years, the emergence of cashless payment methods such as electronic money (E-Money) [1] and quick response code Indonesian standard (QRIS) have played a significant role in driving this growth [2]. These convenient payment methods have made financial transactions faster and more accessible but have also become attractive targets for cybercriminals.

The increasing reliance on digital platforms, driven by these innovations, demands a collective effort to build a robust cybersecurity framework [3]. While advancements in digital payments address the need for convenience, the human element remains a critical weak link in the fight against cyber threats.

Cybersecurity is often considered a technological problem, but human factors play a crucial role [4]. Many cyberattacks stem from human error, opening unknown attachments and clicking malicious links [5]. Hackers frequently target sensitive financial information, including company data, transaction records, and personal client details [6]. Accounting and finance professionals are particularly vulnerable, as the data they manage makes them prime targets for cyberattacks in the digital environment. Cyberattacks like hacking and identity theft can result in reputational damage, privacy violations, and severe

*Author for correspondence

financial losses [7]. Therefore, enhancing cybersecurity awareness among accounting and finance students is an essential precaution.

Several studies have been conducted to develop cybersecurity awareness programs. Research by Fadlika et al. [8] A traditional educational approach with direct interaction and guided discussions is effective in increasing understanding but is limited by the need for physical presence. Research by Yeoh et al. [9] showed that awareness campaigns can increase awareness temporarily but are less effective in maintaining long-term effects. Research with the capture the flag (CTF) Approach conducted by Fisk [10] It proved effective for participants with technical backgrounds but needed to be more suitable for fields such as accounting and finance. Meanwhile, research with virtual reality-based methods conducted by Rana and Chicone [11] showed great potential, but faced accessibility constraints and high resource requirements.

Alternatively, mobile learning offers a more efficient solution regarding accessibility and resources. Utilising devices such as smartphones and tablets are a cost-effective option. Several previous studies have shown that mobile learning has been efficacious in improving learning outcomes [12], comprehension [13], motivation [14], knowledge retention [15], and practical skill [16]. This approach has been used in various disciplines [17]. The interactive and personalised delivery of content makes it promising for overcoming he limitations of previous cybersecurity awareness programs. Based on several studies, a research gap related to mobile-based learning approaches to increase cybersecurity awareness, especially for accounting and finance groups.

This study aims to address the identified gap by evaluating the effectiveness of a mobile learning-based cybersecurity program in enhancing cybersecurity awareness among accounting and finance students. The findings have the potential to transform cybersecurity education by offering a flexible, accessible, and effective approach tailored to the unique needs of these students. Additionally, the results can assist educational institutions in developing progressive policies to integrate cybersecurity education into their curricula.

The paper is organized as follows: Section 2 provides a review of existing literature on cybersecurity awareness and mobile learning within the financial sector. Section 3 outlines the research methodology, focusing on the design and implementation of the mobile learning-based program. Section 4 presents the findings and explores their implications for accounting and finance students. Finally, Section 5 concludes the study by summarizing key insights and offering recommendations for future research and educational practices.

2.Literature review

The literature review aims to explore existing studies and approaches related to cybersecurity awareness, particularly in the context of educational technology. This section examines various methods used to enhance cybersecurity knowledge, highlighting their strengths and limitations. By identifying gaps in prior research, this review provides a foundation for developing and evaluating the proposed mobile learning-based cybersecurity awareness program.

Cybersecurity awareness programs are critical to mitigating risks associated with human factors in cybersecurity breaches. As cyber threats evolve and become more sophisticated, the role of human error in these breaches can no longer be underestimated [18]. Research has shown that the majority of cybersecurity incidents stem from human actions [19], such as falling victim to phishing attacks [20], mishandling sensitive information [19], or failing to follow basic security protocols [21] . These human-related vulnerabilities underscore the critical need for comprehensive cybersecurity awareness programs that educate and empower individuals to recognise and respond effectively to potential threats.

Addressing human factors in cybersecurity breaches requires comprehensive awareness programs that educate individuals on recognizing and mitigating digital threats. Various approaches have been explored to address this need, each with distinct methodologies, results, advantages, and limitations. Security awareness campaigns, which commonly utilise mass communication strategies such as emails, posters, seminars, and courses, have been shown to increase awareness levels temporarily [22]. Research by Georgiadou et al. [23] highlights their effectiveness in raising employee awareness, but the impact tends to decline over time unless continuous reinforcement is provided. Similarly, Lee and Choi [24] research findings suggest that cyberattack campaigns are easy to implement and can increase participant awareness. Likewise, the findings of research conducted by Vrhovec et al. [25] state that campaigns are a concise way to increase

cybersecurity awareness. However, while these campaigns are easy to implement and can quickly reach a broad audience, their short-lived effect limits their sustainability as a long-term solution.

Another approach is the traditional classroom-based program, which includes lectures, workshops, and practical exercises, providing a more structured learning environment. Such as research conducted by Balogun et al. [26] where the research findings revealed that these programs have been proven to improve cybersecurity knowledge and skills. In addition, Childers et al. [27] also revealed that integrating cybersecurity lessons into the curriculum can prevent students from cyber attacks. Another study conducted by Wusylko et al. [28] revealed that the use of comics to improve understanding of cryptography and cybersecurity has a positive impact. However, this approach has limitations in the level of engagement and retention remains a significant challenge. The static nature of these programs can fail to capture the dynamic and evolving cybersecurity threats. Additionally, they often need more personalization, making it easier to address the diverse learning needs of participants with varying levels of prior knowledge or expertise. Despite offering interactive discussions and practical exercises, their effectiveness could be improved in foster sustained learning.

Interactive methods like CTF competitions present an alternative by engaging participants in solving cybersecurity challenges in a competitive format. Studies by Kim et al. [29] demonstrate that CTF competitions are highly effective for participants with technical backgrounds, as they foster critical thinking, problem-solving abilities, and hands-on experience. However, research by Purbo et al. [30] notes that these competitions are more suitable for more technical audiences, such as accounting and finance students, due to the prerequisite of technological expertise. This limitation restricts their broader applicability.

Emerging trends in cybersecurity education focus on integrating artificial intelligence (AI) and machine learning to deliver personalised learning experiences. Research findings by Ortiz-garcés et al. [31]. suggest that AI-based systems can adapt to an individual's pace and learning style, significantly improving efficiency and retention in raising cybersecurity awareness. These systems leverage real-time data to deliver customized content, ensuring learners are engaged and receive targeted support. Furthermore, research by Reddy et al. [32] suggests that these systems can simulate complex cyber scenarios, providing hands-on experience in a controlled environment. Research by Soon et al. [33] also leverages AI by simulating phishing attacks to test the safety awareness of social media users. Even more sophisticated, Mishara et al. [34] suggests that AI can be used to detect cyberattacks. However, the complexity and cost of developing such systems present challenges to widespread adoption, especially in resource-constrained environments.

The reviewed studies highlight the strengths and weaknesses of these diverse approaches. Security awareness campaigns and traditional classroom-based programs offer structured and scalable solutions but often lack engagement and sustained impact. Meanwhile, interactive methods like CTF competitions and game-based learning provide high engagement and skill development but are resource-intensive and unsuited for non-technical learners. AI-based personalised learning systems have transformative potential but face practical challenges related to cost and complexity. Despite these advancements, a critical gap remains in developing accessible, scalable, cost-effective cybersecurity awareness programs tailored to non-technical learners, mainly accounting and finance students. This review highlights the need for a flexible, accessible, and scalable solution to bridge cybersecurity awareness gaps among accounting and finance students. Mobile learning offers a way to bridge this gap by delivering cost-effective, interactive, and flexible content tailored to the unique needs of this audience.

3.Method

This study employed a developmental research methodology to design, develop, and evaluate a mobile learning-based program aimed at enhancing cybersecurity awareness among vocational accounting and finance students. Developmental research focuses on the creation and refinement of educational tools and interventions through a systematic process of analysis, design, and evaluation [35]. The aim is to create practical solutions that effectively increase cybersecurity awareness among the target audience.

3.1Research procedures

The research procedure follows the 4D model, which consists of four stages: Define, Design, Develop, and Disseminate. This model provides a structured approach to the development and implementation of

educational programs [36]. The research steps are illustrated in *Figure 1*.

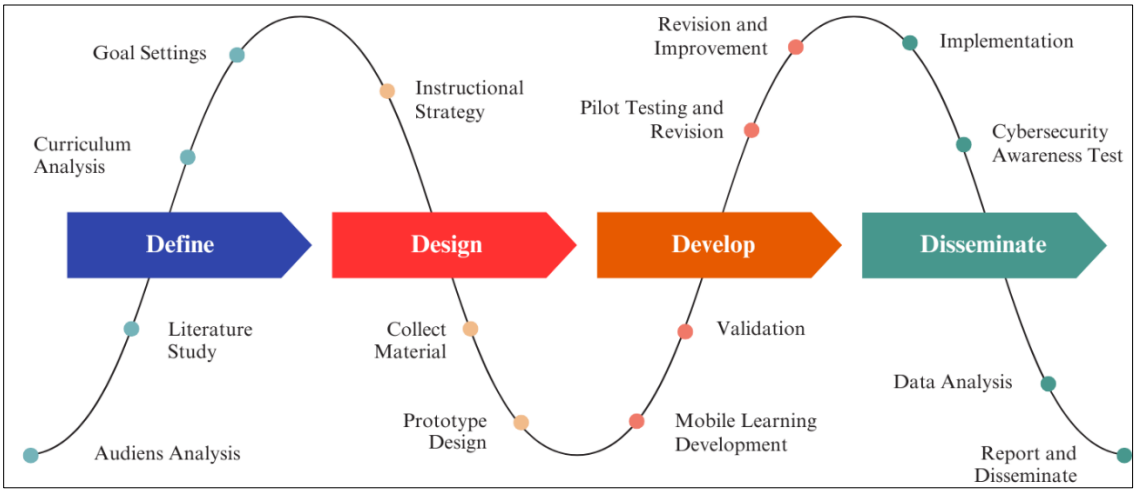

Figure 1 Stages in the research procedure

The define phase is the cornerstone of the development process, focusing on identifying and understanding the target audience's specific needs. This begins with a comprehensive needs analysis, where a thorough literature review is conducted to find gaps in existing cybersecurity awareness programs. By analyzing these gaps, a clearer understanding of the unique challenges faced by vocational accounting and finance students, particularly in the context of cybersecurity, can be achieved. Additionally, data was collected through interviews and surveys with educators and students to gain insights into their experiences, challenges, and expectations regarding cybersecurity education. This analysis helps identify characteristics such as the current level of knowledge, learning preferences, and technology proficiency. Curriculum analysis was also carried out to determine the extent to which cybersecurity education was taught and which strategies and media were employed. Based on these insights, clear learning objectives are established to guide program design and development, ensuring the program is tailored to meet participants' specific needs and goals.

The design phase focuses on conceptualizing the structure and content of a mobile learning-based cybersecurity awareness program. Appropriate teaching strategies are selected to align with the learning objectives and the needs of the target audience. Interactive and engaging learning activities, such as quizzes, simulations, and case studies, are designed to enhance knowledge retention and practical skills. Detailed storyboards and mobile learning module prototypes are created to visualize the content and user experience. Ensuring usability is crucial during this phase, as the design must be user-friendly and accessible across various mobile devices. Feedback mechanisms are integrated to support iterative design improvements, enabling adjustments based on user feedback and testing results. This phase lays the foundation for developing a robust and effective learning program.

The development phase transforms the prototype into a functional mobile learning module. This requires collaboration with instructional designers, software developers, and subject matter experts to ensure the content is accurate, relevant, and technically sound. The development process includes iterative cycles of testing and refinement to address issues and enhance the module's quality. Pilot testing was conducted with a small group of students to gather initial feedback on usability and effectiveness, allowing for further revisions and improvements based on real-world use. The iterative nature of this phase ensures that the final product aligns with the stated learning objectives and user needs, resulting in a high-quality educational tool designed to enhance cybersecurity awareness among vocational accounting and finance students.

The dissemination phase focuses on implementing and evaluating programs developed on a larger scale. The mobile learning-based cybersecurity awareness program was applied to a broader audience of vocational accounting and finance students, with training and support provided to educators and

students to facilitate implementation. Data was collected through pre- and post-assessment surveys, focus groups, and usage analysis to evaluate the program's impact on students' cybersecurity knowledge, attitudes, and behavior. The findings are analysed to assess the program's effectiveness and identify areas for further improvement. Finally, the results and insights obtained from the evaluation are disseminated through academic publications, conferences, and collaboration with educational institutions. This promotes the adoption of the program and fosters further research and development in cybersecurity awareness education, thereby contributing to the overarching goal of enhancing cybersecurity practices in the financial sector.

3.2Research subject

The subjects of this research involved vocational high school students in accounting and finance, who were from several vocational high schools in Yogyakarta, Indonesia. The total research participants were 136 students. The subjects were selected using convenience sampling, where schools that agreed to participate in the study provided access to their accounting and finance students. This approach was chosen due to logistical considerations and the willingness of schools to collaborate. The choice of sampling method ensured that the participants were relevant to the research topic, which focuses on increasing cybersecurity awareness in the context of accounting and finance education. The research design used in this study is pretest and posttest as shown in *Figure 2*.

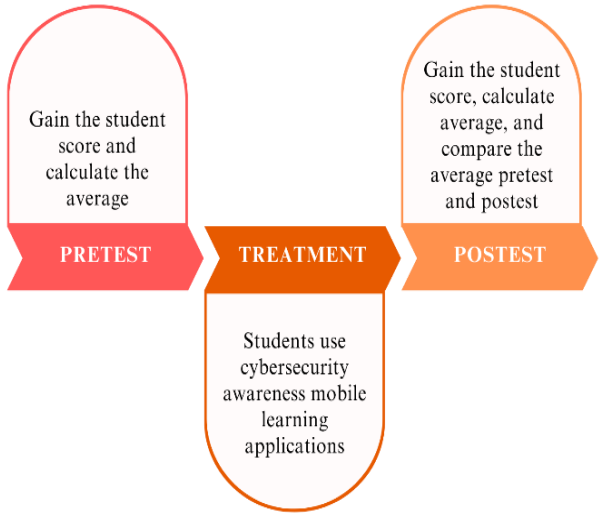

Figure 2 Pretest and posttest design to evaluate program effectiveness

In this design, each group of students takes a pretest to assess their initial knowledge and awareness of cybersecurity prior to the intervention. Subsequently, they participate in a mobile-based learning program aimed at enhancing cybersecurity awareness. Upon completing the program, a posttest is administered to evaluate the changes in students' knowledge and awareness. This design allows researchers to measure the program's effectiveness by comparing pretest and posttest results and identifying improvements due to the intervention. Given that the main focus of this study was to evaluate the direct impact of the mobile learning application on the studied group, this study did not use a control group.

3.3Research instrument and data analysis

3.3.1Validity instrument

This instrument assesses the mobile learning module's content and construct validity. Cybersecurity and educational technology experts review modules to ensure the content is accurate, relevant, and aligned with learning objectives. Validity instruments help identify and address content gaps or inaccuracies. The indicators used are available in *Table 1*.

Table 1 Indicators for validity assessment of the instrument

Indicator	No. item
Curriculum alignment	1 - 3
Functional	4 - 7
Performance	8 - 12
Safety	13 - 16
Appearance	17 - 20

Validity testing by experts was conducted using Aiken's V validity coefficient calculation method, a widely recognized approach for evaluating the accuracy of research instruments. The calculation is presented in Equation 1.

$$V = \frac{\sum(r_i - r_x)^2}{k(k+1).(N-1)} \quad (1)$$

Description:
V = Coefficient Validity
r_i = Correlation between the scores of each expert
r_x = Average of all correlations between experts
k=The total number of experts who provided assessments
N=Number of items or questions in the research instrument

The results of each expert's validity evaluation were then collected and analyzed to assess the extent to

which this instrument complies with established standards. The cybersecurity awareness program that has been prepared is considered valid if all experts meet the previously established criteria. The validity criteria used as a reference can be found in *Table 2*.

Table 2 Criteria for assessing validity of instruments

Criteria	Description
≥0.6	Valid
<0.6	Invalid

3.3.2Reliability instrument

The reliability of the instruments used in this study was assessed to ensure that they consistently measure cybersecurity awareness among the participants. Reliability testing was conducted using Cronbach's alpha, a widely used statistical measure for evaluating the internal consistency of a set of items. Cronbach's alpha is calculated using the Equation 2.

$$\alpha = \frac{N.c}{v+(N-1).c} \quad (2)$$

Description:
α = Cronbach's alpha coefficient
N= Number of items in the test
c = Average covariance between item pairs
v = Average variance of each item

Before the main study, a pilot test was conducted with 30 Vocational High School student's representative of the target population. According to established guidelines, Cronbach's alpha values are interpreted as shown in *Table 3*.

Table 3 Cronbach's alpha reliability classification

Range	Description
> 0.90	Excellent reliability
0.80 – 0.89	Good reliability
0.70 – 0.79	Acceptable reliability
0.60 – 0.69	Questionable reliability
0.50 – 0.59	Poor reliability
< 0.50	Unacceptable reliability

The Cronbach's alpha value obtained was 0.85, which falls within the Good Reliability range. This result indicates that the instrument has internal solid consistency and is suitable for assessing cybersecurity awareness.

3.3.3Cybersecurity awareness test

Standardized tests were administered to the experimental and control groups to objectively evaluate their cybersecurity knowledge and skills. These multiple-choice questions require students to demonstrate understanding and application of cybersecurity practices. The tests given previously have passed tests for validity, reliability, distinguishing power, and difficulty level. Average test results were compared between the experimental and control groups to determine the effectiveness of the mobile learning-based approach. Equation 3 is used to calculate the average value.

$$NA = \frac{S}{M}\ x\ 100\% \quad (3)$$

Description:
NA = Final Score
S = Score obtained
M = Maximum score

Next, the pretest and posttest results were analysed using the Gain score, which measures the difference between the pretest and posttest scores (Equation 4).

$$< g >= \frac{(\%<Sf>-\%<c>}{(100-\%<Si>} \quad (4)$$

Description:
g = gain score
Sf = posttest score
Sf = pretest score

The gain score measures the difference between students' comprehension scores before and after participating in a cybersecurity awareness program. The effectiveness of the program in improving student understanding can be determined by analyzing the scores obtained. If the score reaches the "medium" or even "high" category, the program has succeeded in providing new knowledge or improving existing understanding. On the other hand, if the score only reaches the "low" category, this may indicate that the program needs to be revised or improved to achieve better results. The criteria for gain values are presented in *Table 4*.

Table 4 Criteria for gain score interpretation

Gain Score	Interpretation
(<g>) > 0,7	High
0,7 > (<g>) >0,3	Medium
(<g>) < 0,3	Low

3.3.4Effectivity instrument

The cybersecurity awareness test is designed to evaluate the extent to which students have internalized the cybersecurity concepts taught during the program. It assesses behavioral changes related to cybersecurity practices following participation in the awareness program. Test evaluates various aspects, including the use of strong passwords, adoption of security software, awareness of cyber threats, and

implementation of other preventive measures, through a structured questionnaire. This questionnaire was compiled based on indicators used by several previous studies, namely research by [37–41]. The details are provided in *Table 5*.

Table 5 Indicators for cybersecurity awareness test

Indicator	No. item
Passwords and Access control	1,2,3,4,5
Software and Hardware Security	6,7,8,9,10
Mail and Data Protection	11,12,13,14,15
Network Security	16,17,18,19,20
Data Backup and Recovery	21,22,23,24,25
Encryption	26,27,28,29,30

Next, the instrument is analysed, and the data obtained is compared with the effectiveness category. At this stage, the scores obtained from questionnaire analysis will be compared with predetermined criteria to determine the level of program effectiveness. These criteria cover a range of categories from "Very Effective" to "Ineffective." By comparing the analysis results with the predetermined effectiveness categories, it will be possible to know the extent to which the program successfully achieves the predetermined goals. The details are provided in *Table 6*.

Table 6 Categories effectiveness of cybersecurity awareness program

Indicator	Criteria
85-100	Very Effective
75-84	Effective
60-74	Moderately Effective
55-59	Les Effective
0-54	Not Effective

4.Result and discussion

4.1Design

In the design phase, the activities include developing an initial design that comprises a data flow diagram (DFD) to illustrate the flow of data within the system, an entity-relationship diagram (ERD) to map the relationships between entities in the database, and a system work design (SWD) that outlines the structure and overall system workflow. This comprehensive design ensures that all system components are seamlessly integrated and operate according to the specified requirements, thereby facilitating effective and efficient program implementation.

4.1.1Data flow diagram (DFD)

DFD is designed to describe the flow of data and the processes in the system, where two external entities interact with it: students and instructors. Students interact with the entire mobile learning system, while the instructor acts as a companion and guide for students in learning with mobile learning. The context diagram and DFD are shown in *Figure 3* and *Figure 4*, respectively.

Figure 3 Context diagram interaction between users and system components

The process starts from the start stage, where the user opens the application. Users are then directed to the introduction page, which provides an overview of the purpose and benefits of cybersecurity awareness programs. After that, the system checks the cache to see whether the user has logged into the application. The user is immediately directed to the main page if there is cache data. Users must always go through the login page to log in using their credentials if there is no cache data. After successfully logging in, users arrive at the main page, which functions as a navigation center for various features and learning content. On this main page, users can access multiple lesson pages, divided into five sections, each containing learning material presented through text, video, animation, simulation, and quizzes to measure understanding.

After completing all learning modules, users must undergo a comprehension test to assess the extent of their understanding of the material they have studied. Once the test is complete, the user will reach Finish, where they can see the results and feedback. This application also provides a discussion feature that allows users to interact and discuss topics related to cybersecurity. The create discussion button enables users to create a new discussion topic, while several previously created discussion topics are below it. This DFD provides a clear picture of how users interact with the application and its various elements and stages.

4.1.2Entity relationship diagram (ERD)

The ERD from a mobile learning application for a cybersecurity awareness program depicts the relationship between various entities in the system. The ERD is shown in *Figure 5*.

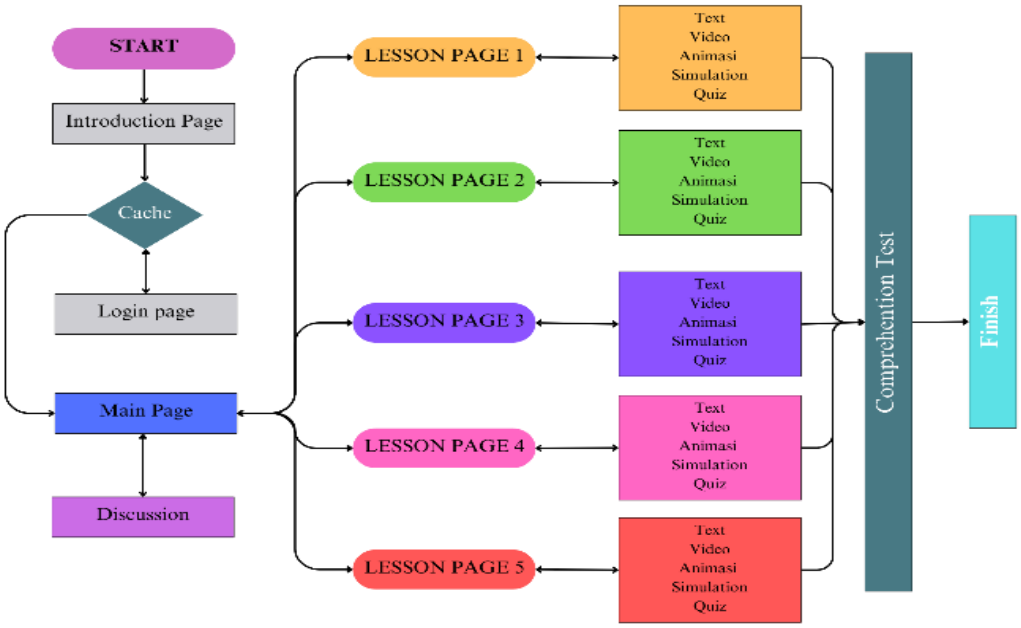

Figure 4 DFD of cybersecurity awareness application

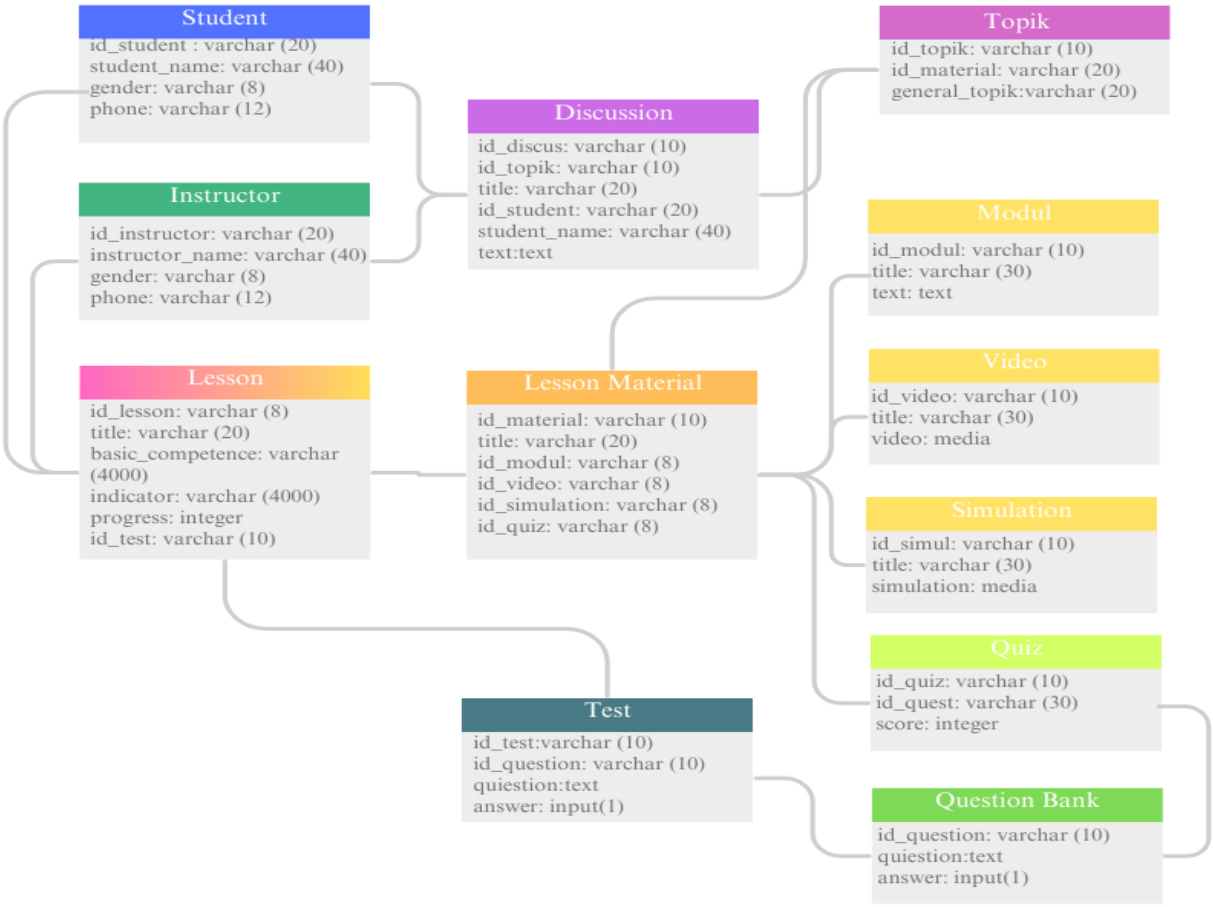

Figure 5 Entity Relationship diagram of cybersecurity awareness application

The main entities in this diagram include the Student, Instructor, Lesson, Lesson Material, Discussion, Topic, Module, Video, Simulation, Quiz, Test, and Question Bank. The student entity has attributes such as id_student, student_name, gender, and phone, through which each student can participate in discussions and access course materials. Instructors with the attributes id_instructor, instructor_name, gender, and phone are responsible for providing and managing lesson content. Lessons contain information about lessons with attributes such as id_lesson, title, basic_competence, indicators, progress, and id_test and are related to lesson material consisting of various types of content. Lesson material has the attributes id_material, title, id_modul, id_video, id_simulation, and id_quiz. The Discussion entity handles discussion topics created by students with the attributes id_discus, id_topic, title, id_student, and student_name. Topics, with the attributes id_topic, id_material, and general_topic, indicate materials related to a specific topic.

The module consists of the id_modul, title, and text attributes, representing the learning module, while the Video entity has the id_video, title, and video attributes, which store information about the learning video. The simulation contains id_simul, title, and simulation, describing the simulation used in the lesson material. Quizzes consist of the attributes id_quiz and id_quest, with links to a question bank for storing questions. The test contains id_test, id_question, and score, which connects the test with a question bank to store questions and scores. Finally, the Question Bank consists of id_question, question, and answer, which stores all the questions and answers used in quizzes and tests. This ERD provides a comprehensive picture of how the various entities in the mobile learning application relate to each other and interact to support cybersecurity awareness programs.

4.1.3System work design (SWD)

This mobile learning application's SWD for cybersecurity awareness describes the communication workflow between server components and user devices. The SWD is shown in *Figure 6*. At the top are two main servers: application server and database server. The application server is responsible for processing application logic and managing user requests. At the same time, the database server stores and manages the data required by the application, such as user information, study materials, and test results. These two servers communicate with each other continuously to ensure the data displayed to users is always up to date.

Communication between the server and user devices is carried out over the internet network, symbolised by the cloud icon and wireless fidelity (Wi-Fi) signal in the center of the diagram. The user's device, in this case a smartphone, is connected to the application server via the internet. When a user opens an application and performs activities such as logging in, accessing study materials, or taking a test, these requests are sent to the application server. The application server then processes the request and, if necessary, retrieves data from the database server. The processing results are returned to the user's device via the Internet.

This workflow design ensures that users from various locations can access the mobile learning application with an internet connection. The use of two separate servers also helps optimise application performance. The application server focuses on processing application logic, while the database server handles data management. Thus, users can enjoy a smooth and efficient learning experience supported by a robust and well-managed infrastructure.

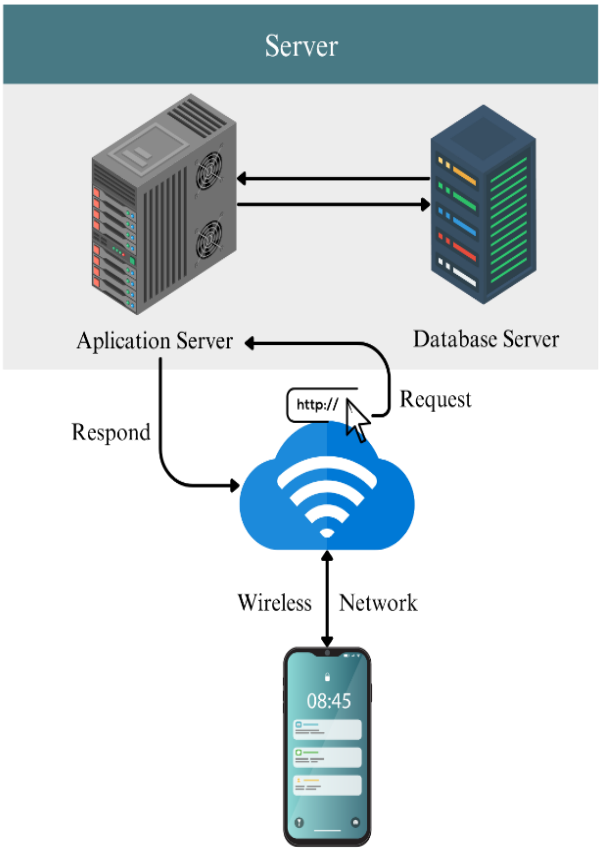

Figure 6 Systems work design: communication flow between server and user device

4.2Develop

In this stage of the cybersecurity awareness program, we developed learning content specifically designed for accounting and finance. The application covers five lessons: an introduction to cybersecurity, password and access control, software and hardware safety, mail and data protection, network safety, data backup and recovery, and data encryption.

4.2.1Introduction page

Displays At the top of the screen is the text "CYBERSECURITY AWARENESS PROGRAM," presented in bold blue font, emphasising this application's title and primary purpose. Below the title, there is an interesting visual illustration: a character with a hacker-like appearance. This illustration is surrounded by icons depicting important aspects of data security, such as information protection, cyber threats, and the technological components involved. Right below the illustration, there is the text "DATA SECURITY START WITH YOU" followed by "PROTECT YOUR CAREER, CLIENT, YOUR REPUTATION," which gives a firm message that data security starts from individual awareness and actions, as well as the importance of data protection in protecting careers, clients, and reputation. The bottom of the screen displays two interactive buttons with the text "GET STARTED," inviting users to start a cybersecurity awareness program. The second button has the text "GET HACK," which provides a contrasting option that warns users of the risks of not following the program. This design was created to attract attention and encourage users to start the program immediately to secure their data. Overall, this “Introduction” display is designed to attract users' attention, provide an understanding of the importance of cybersecurity, and motivate them to take action by starting the cybersecurity awareness program offered. The introduction page display is shown in *Figure 7*.

4.2.2Main page

Display of the main page of the application "Cybersecurity Awareness Program." At the top of the screen is a personal welcome with the text "Welcome back, Radinal Fadli!" which gives application users a sense of personalization. The greeting is presented on a panel featuring an illustration of the same hacker character as displayed on the introduction page. This panel contains the invitation "Start Learning Today to Level Up Your Security," written in upper- and lower-case letters to attract attention and motivate users to start learning immediately. The main section of the page consists of several buttons, each representing a different learning topic in a cybersecurity awareness program. Each button includes a topic title and an indicator of student learning progress. The main page display is shown in *Figure 8*.

Figure 7 Introduction page: overview of cybersecurity awareness program

Figure 8 Main page: navigation center for cybersecurity learning topics

4.2.3Lesson page

This is the learning page for the "Cybersecurity Introducing" module in the "Cybersecurity Awareness Program" application. At the top of the screen is a heading, "CYBERSECURITY INTRODUCING," emphasizing the studied topic (*Figure 9*). Videos that can be played provide visual and audio explanations of the issues discussed. In addition, there is text that provides a detailed explanation of cybersecurity.

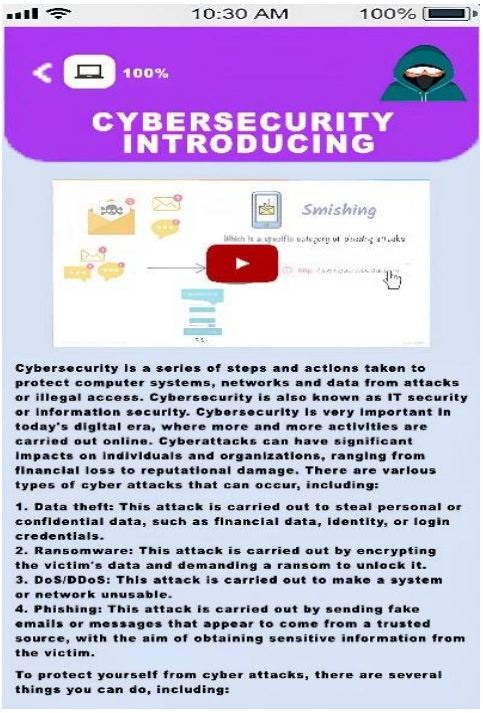

Figure 9 Lesson page: content structure for cybersecurity introduction module

4.2.4Simulation page

The "simulation" page is displayed in the "Cybersecurity Awareness Program" application. At the top of the screen is the title "Mail Phishing," which indicates the section of the simulation the user is accessing. The title, "Simulation," suggests the user is in simulation mode for this application. The central part of this page consists of a simulated display of an email that looks like an actual email. This email is designed to resemble the phishing emails typically used by hackers to trick users into clicking on malicious links. The emails contain content such as urgent messages asking users to update their account information or confirm unknown transactions. A phishing link is included, where users can click on the link, triggering a simulation that demonstrates the consequences of such an action. Users are redirected to a fake page designed to mimic a legitimate website, which prompts them to enter sensitive information, such as their username and password. This simulation provides a first-hand experience of how a phishing attack can occur and what users should be aware of. The simulation page is shown in *Figure 10.*

Figure 10 Simulation page: phishing email examples and interactive features

4.2.5Discussion room

The "Discussion Room" page in the application "Cybersecurity Awareness Program." At the top of the screen is a button with the text "Create Discussion." This button allows users to create new discussion topics, encouraging interaction and collaboration between users in discussing cybersecurity-related issues. Several discussion topics have been made under the "Create Discussion" button. Each discussion topic is displayed with a clear title. Users can click on the topic title to enter the discussion, read existing comments, and add their opinions or questions. With this "Discussion Room" feature, the "Cybersecurity Awareness Program" application provides one-way learning material and an interactive platform where users can share knowledge, exchange experiences, and help each other understand and overcome cybersecurity challenges. This aims to create a community that is active and aware of the importance of maintaining security in the digital world. The discussion page display is shown in *Figure 11.*

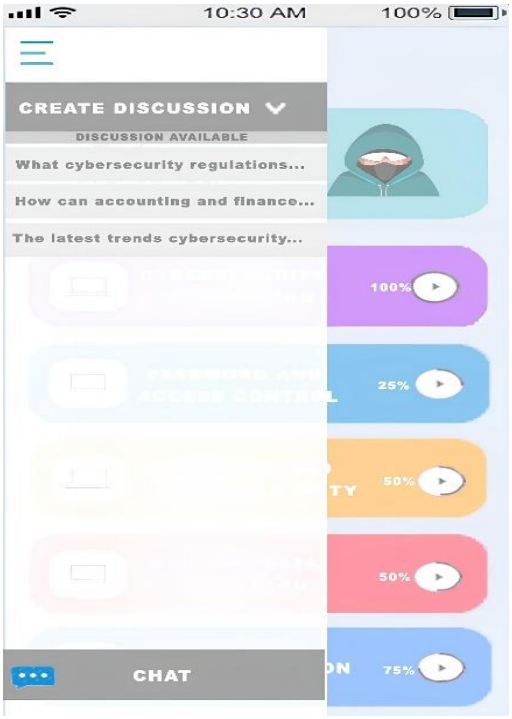

Figure 11 Discussion room: interactive platform for cybersecurity topics

4.3Develop

4.3.1Validity result

Validity is essential in development research to ensure that the instruments and materials used are fit for purpose and reliable. This validity testing process involves an evaluation from 3 competent experts in cybersecurity and education, who assess the content and program design's quality, relevance, and effectiveness. Validity testing was conducted, and the results are presented in *Figure 12*.

Assessment of the "Curriculum alignment" indicator received an average score of 0.8, indicating that this program follows the established curriculum and is relevant to students' learning needs. The "Operational" indicator also received an average score of 0.8, indicating that the program can operate well and has clear user instructions. Furthermore, the "Performance" indicator obtained an average value of 0.8, which shows that this program can provide exemplary performance in delivering learning material and achieving the desired goals. The “Security” indicator, which is very important in cybersecurity, received the highest average score of 0.9, indicating that the program meets high-security standards and can be relied on to protect user information. Finally, the "Design" indicator gets an average score of 0.8, indicating that the interface design of this program is well-designed, attractive, and easy for students to use. Overall, all indicators evaluated by the validators show that this program is valid and can be used as a practical learning tool in increasing cybersecurity awareness among vocational school students in accounting and finance.

4.3.2Pilot testing and revision

After going through the validity stage, this mobile learning-based cybersecurity awareness program entered the initial testing or pilot testing stage. This activity was conducted in small groups of vocational school students in accounting and finance. The primary purpose of pilot testing was to ensure that the application could function effectively under various conditions and on different student devices. Pilot testing involved a range of devices with varying specifications to ensure broad compatibility, including Android-based devices with other operating system versions. During testing, participants were asked to operate the application, follow the learning modules, and complete the simulations and tasks provided.

The results of pilot testing showed that the application performed well on various devices and operating conditions. No significant errors or technical issues were encountered during usage. Interaction and navigation within the application ran smoothly, ensuring that users could easily access and utilise all features.

In addition to technical performance, qualitative feedback from participants provided valuable insights into the user experience. Several students highlighted the application's usability, noting that it was easy to navigate and user-friendly. One participant remarked, "The menus and modules are straightforward, and it was easy to find what I needed without confusion." Another student mentioned the visual design: "The interface is simple but engaging, and the colours make the learning process enjoyable."

Regarding engagement, participants expressed appreciation for the interactive simulations and tasks. One student said, "The simulations make it feel like I’m solving real-world problems, which helps me understand the concepts better." Another added, "The quizzes at the end of each module kept me motivated to keep learning and test my knowledge."

In terms of content relevance, students perceived the material as directly applicable to their field. A participant commented, "The examples and scenarios related to accounting and finance make the content

relevant to my studies." Another noted, "I never thought about cybersecurity in this way before, but now I understand how important it is for my future career."

Based on this feedback, several minor revisions were made to enhance the user experience further. These included interface adjustments to improve navigation, minor improvements to interactive features, and optimisation to increase access speed in specific modules.

Thus, the pilot testing results and subsequent revisions demonstrate that the application is ready for broader implementation. The feedback indicates that the mobile learning application provides an effective and engaging solution for increasing cybersecurity awareness among vocational school students in accounting and finance.

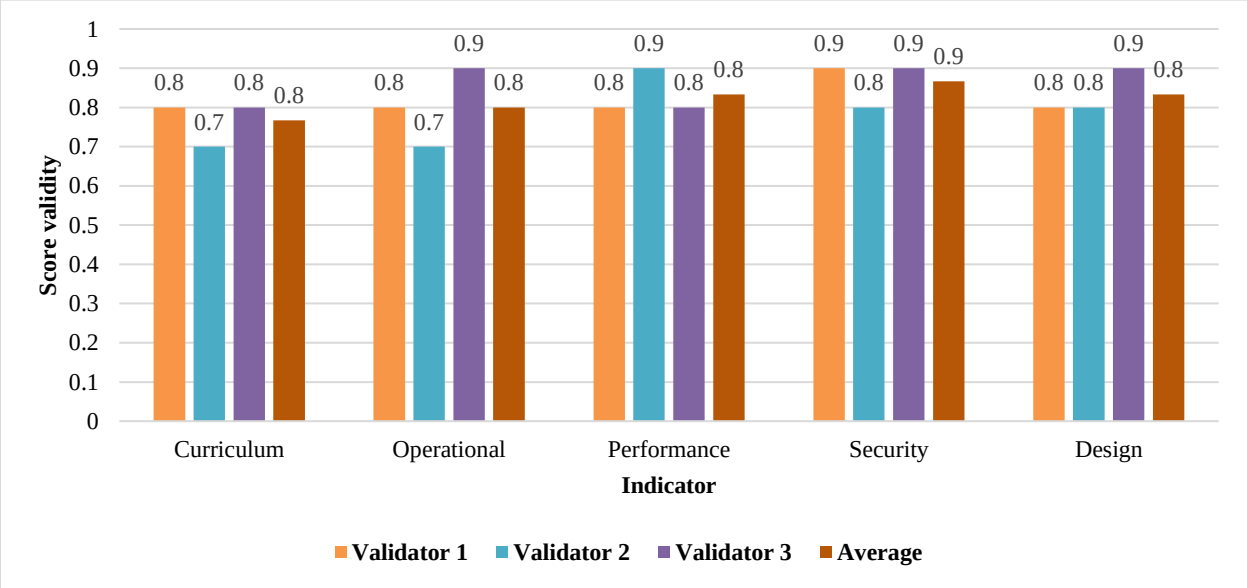

Figure 12 Cybersecurity awareness application validity results

4.4Disseminate

4.4.1Cybersecurity awareness test

After the cybersecurity awareness mobile learning application was applied to vocational school students in accounting and finance, an understanding improvement test was carried out to determine how much this program could improve students' understanding of cybersecurity. The students' overall scores, obtained after the test, are presented in *Table 7*.

Table 7 Cybersecurity awareness test gain score summary

N	Gain score minimum	Gain score maximum	Gain score
136	0.50	0.93	0.72
Category			High

Based on the gain score results, the minimum gain score data was obtained at 0.50 and the maximum gain score at 0.93, with an average gain score of 0.72. This gain score shows how much the student's understanding has increased after following the learning program. The average gain score of 0.72 is in the high category, indicating that this mobile learning application is practical in improving students' understanding of cybersecurity. So, this security awareness application with mobile learning can increase the security awareness of vocational school students in accounting and institutional finance expertise by 72%. This significant increase shows that a mobile learning-based learning approach can increase students' awareness and understanding more effectively than traditional methods. With interactive features and relevant content, students can more easily understand essential concepts in cybersecurity and apply that knowledge in their daily lives and future work environments. These results also strengthen the findings from pilot testing that this application can function well and provide tangible benefits in the learning process. This finding aligns with previous studies by Samala et al. [42], which demonstrated the effectiveness of mobile learning in enhancing learning outcomes, particularly in improving knowledge retention and engagement. Unlike traditional classroom-based methods, which

often face challenges in maintaining long-term retention, mobile learning is more engaging and accessible for non-technical learners.

4.4.2Effectiveness test

After completing the program, a security awareness questionnaire was given to students to determine how effective the mobile learning-based cybersecurity awareness program is in increasing security awareness. This instrument was given to 136 vocational school students in accounting and finance. Respondents were asked to provide assessments and responses according to the questionnaire. The collected data was analyzed to produce the results presented in *Table 8.*

Table 8 Effectiveness results for cybersecurity awareness program

Indicator	Score	Category
Passwords and Access control	85	Very Effective
Software and Hardware Security	80	Effective
Mail and Data Protection	87	Very Effective
Network Security	80	Effective
Data Backup and Recovery	77	Effective
Encryption	80	Effective

The effectiveness testing of the cybersecurity awareness program using mobile learning demonstrated positive and satisfactory outcomes based on the scores obtained for each indicator. For the password and access control aspect, the program achieved a score of 85, classified as "Very Effective," highlighting its success in promoting adequate password management and access control practices.

In the software and hardware security aspect, the program received a score of 80, categorized as "Effective." Similarly, the mail and data protection indicator showed exceptional results with a score of 87, classified as "Very Effective," reflecting the program's success in emphasizing the importance of secure email and data practices.

Network security, data backup and restore, and encryption scored 80, 77, and 80, respectively, all falling within the "Effective" category. These scores indicate the program's success in fostering cybersecurity-related skills and practices.

With consistent results ranging from the "Effective" to "Very Effective" categories, this study highlights the potential of mobile learning as a viable solution to address the limitations of CTF approaches. By offering a more straightforward yet effective method to improve cybersecurity awareness, the mobile learning program leverages interactive features and contextually relevant content to motivate safer behavioral changes and enhance practical skills, particularly for non-technical learners.

4.5Discussion

This research produces a mobile learning-based cybersecurity awareness program that effectively increases cybersecurity awareness among accounting and finance vocational school students. The validity test results show that the mobile learning application developed has been well received by cybersecurity and educational technology experts, with an average validity value reaching 0.8 or higher for each indicator tested. Specifically, aspects of curriculum, operations, performance, security, and application design are considered valid for cybersecurity education.

Significant improvements were also seen in students' understanding of cybersecurity, which was reflected in increased understanding scores before and after implementing the application. The mobile learning-based cybersecurity awareness program has increased knowledge by 72% in various aspects of cybersecurity. The effectiveness of this application has also been proven to be significant based on the evaluation results. Consistent use of this application increases cybersecurity awareness, especially in password management and access control, software and hardware protection, as well as email security and data protection, all of which achieve the "Highly Effective" or "Effective" category.

The findings of this research show several advantages compared to previous research. Compared with research by Taherdoost [43], which used conventional modules in cybersecurity training, the mobile learning application in this research consistently achieved a higher level of effectiveness in increasing students' understanding of cybersecurity aspects. Additionally, research by Hodhod et al. [44], which focuses on game-based learning to increase cybersecurity awareness, shows that these applications provide additional advantages in terms of accessibility and low cost, as evidenced by their ability to operate seamlessly on various devices without using additional devices. Additionally, in research by Ortiz-garces et al. [45], which focused on the CTF competition to hone security skills. This mobile learning application offered a more inclusive approach, where users were not required to have advanced technical skills to use it effectively.

Overall, the findings from this research reinforce that mobile learning applications can be an effective and affordable tool for increasing awareness and understanding of cybersecurity among students. This is supported by previous research by Kim et al. [46], which used mobile learning to increase awareness of work safety in the construction sector.

While these findings are promising, several factors may have influenced the results and should be considered. Among them, participants overestimated their knowledge or provided socially desirable responses, which could affect the results' accuracy—differences in device type and internet speed may affect their engagement with the application. Students using older devices or slow internet connections may experience decreased usability, affecting their learning outcomes. The sample size of 136 may limit the generalizability of the findings to other contexts or populations. Larger-scale studies with more diverse samples, including students from different regions or educational backgrounds, would provide a more comprehensive understanding of the effectiveness of the application. Although the results show significant improvements in understanding, it is uncertain whether these improvements will be sustainable; future studies should include follow-up evaluations of behaviour over a more extended period, providing deeper insight into the long-term impact of mobile learning programs. These findings suggest that mobile learning apps can effectively increase students' awareness and understanding of cybersecurity. This study emphasizes the importance of integrating educational technology relevant to the needs of today's workforce, where cybersecurity is increasingly a top priority. However, addressing the identified limitations and conducting further comparative research across different learning methods would increase the robustness and applicability of these findings.

A complete list of abbreviations is listed in *Appendix I.*

5.Conclusion and future work

This research has successfully developed a mobile learning-based application to enhance cybersecurity awareness among vocational accounting and finance students. The findings demonstrate a significant improvement in students' understanding of critical cybersecurity concepts. This underscores the effectiveness of mobile learning as a flexible, accessible, and cost-effective approach to addressing cybersecurity education gaps, particularly for non-technical learners. The results highlight the importance of integrating cybersecurity awareness programs into vocational education curricula. The application has proven to be an effective tool for fostering students' understanding of password management, data protection, and network security, which are essential skills for their future careers. Future research should focus on assessing the long-term retention of cybersecurity knowledge among students who use mobile learning applications. Additionally, expanding the program to other disciplines or regions could provide a broader understanding of its applicability.

Acknowledgment

None.

Conflicts of interest

All authors state that no conflicts of interest influenced the results and conclusions presented in the research and development of mobile learning applications to increase cybersecurity awareness. All aspects of the research were conducted independently and objectively, without any influence from outside parties with personal, financial, or commercial interests that could affect the integrity and validity of the findings.

Data availability

Due to privacy and ethical considerations, detailed datasets containing sensitive information cannot be shared publicly. However, anonymized data used for statistical analysis and interpretation in this study can be made available to researchers upon reasonable request from authors who meet the criteria for access to confidential data, following institutional and ethical guidelines.

Author's contribution statement

Fivia Eliza: Writing, funding, resources, validation, visualization, revision, and English grammar correction. **Radinal Fadli:** Idea, writing, software, data collection, implementation, data analysis, and result interpretation. **Yayuk Hidayah:** Project administration, validation, and data curation. **Herman Dwi Surjono:** Supervision, conceptualization, investigation, and analysis. **Ratna Candra Sari:** Supervision, conceptualization, investigation and analysis.

References

[1] Anas T, Cahyawati E. Strategic investment policies for digital transformation. Journal of Southeast Asian Economies. 2023; 40(1):96-126.

[2] Sofwatunnisa AA, Kartawinata BR, Akbar A, Pradana M, Putra A, Hidayat AM. Quick response code as a game-changer of Indonesian digital transactions. WSEAS Transactions on Computer Research. 2023; 11:479-85.

[3] Alshboul Y, Al. Hamouri N. Cybersecurity antecedents of trust: toward OPS adoption in Jordan.

International Journal of Information and Decision Sciences. 2023; 15(1):73-93.
[4] Shah MU, Iqbal F, Rehman U, Hung PC. A comparative assessment of human factors in cybersecurity: implications for cyber governance. IEEE Access. 2023; 11:87970-84.
[5] Nganga A, Scanlan J, Lützhöft M, Mallam S. Enabling cyber resilient shipping through maritime security operation center adoption: a human factors perspective. Applied Ergonomics. 2024; 119:104312.
[6] Kuttiyappan D. Improving the cyber security over banking sector by detecting the malicious attacks using the wrapper stepwise Resnet classifier. KSII Transactions on Internet & Information Systems. 2023; 17(6), 1657-73.
[7] Šijan A, Viduka D, Ilić L, Predić B, Karabašević D. Modeling cybersecurity risk: the integration of decision theory and pivot pairwise relative criteria importance assessment with scale for cybersecurity threat evaluation. Electronics. 2024; 13(21):1-14.
[8] Fadlika R, Ruldeviyani Y, Butarbutar ZT, Istiqomah RA, Fariz AA. Employee information security awareness in the power generation sector of PT ABC. International Journal of Advanced Computer Science and Applications. 2023; 14(4):594-603.
[9] Yeoh W, Huang H, Lee WS, Al JF, Mansson R. Simulated phishing attack and embedded training campaign. Journal of Computer Information Systems. 2022; 62(4):802-21.
[10] Fisk N. Developmental challenges: capture the flag and the professionalization of cybersecurity. Human Organization. 2023; 82(1):61-72.
[11] Rana S, Chicone R. The influence of gender and acceptance of VR cybersecurity training platforms. Issues in Information Systems. 2023; 24(1): 93-100.
[12] Zhang H, Zhang J, Wang J, Zhang H. Integrating mobile learning and SPOC-based flipped classroom to teach a course in water supply and drainage science and engineering. Computer Applications in Engineering Education. 2023; 31(3):620-33.
[13] Errabo DD, Ongoco AA. Effects of interactive-mobile learning modules in students' engagement and understanding in genetics. Journal of Research in Innovative Teaching & Learning. 2024; 17(2):327-51.
[14] Al-said K. Influence of teacher on student motivation: opportunities to increase motivational factors during mobile learning. Education and Information Technologies. 2023; 28(10):13439-57.
[15] Hameed AR, Sumari PB. Adoption and continued usage of mobile learning of virtual platforms in Iraqi higher education an unstable environment. International Journal of Information Management Data Insights. 2024; 4(2):100242.
[16] Nikkerdar N, Sepidar KS, Golshah A, Khavid A. Efficacy of a smartphone application as an aid to enhance the instruction of radiographic differential diagnosis of maxillofacial bony lesions. Journal of Dental Education. 2023; 87(5):702-10.
[17] Thaanyane M, Jita T. The use of mobile technology in higher education: implications for students and instructors. Edelweiss Applied Science and Technology. 2024; 8(4):1236-43.
[18] Whitty MT, Moustafa N, Grobler M. Cybersecurity when working from home during COVID-19: considering the human factors. Journal of Cybersecurity. 2024; 10(1):1-11.
[19] Dornheim P, Zarnekow R. Determining cybersecurity culture maturity and deriving verifiable improvement measures. Information & Computer Security. 2023; 32(2):179-96.
[20] Shombot ES, Dusserre G, Bestak R, Ahmed NB. An application for predicting phishing attacks: a case of implementing a support vector machine learning model. Cyber Security and Applications. 2024; 2:100036.
[21] Moskvin DA. Assessing the security of a cyber-physical system based on an analysis of malware signatures. Automatic Control and Computer Sciences. 2023; 57(8):894-903.
[22] Kemp S. Exploring public cybercrime prevention campaigns and victimization of businesses: a bayesian model averaging approach. Computers & Security. 2023; 127:103089.
[23] Georgiadou A, Michalitsi-psarrou A, Askounis D. A security awareness and competency evaluation in the energy sector. Computers & Security. 2023; 129:103199.
[24] Lee I, Choi C. Camp2Vec: embedding cyber campaign with ATT&CK framework for attack group analysis. ICT Express. 2023; 9(6):1065-70.
[25] Vrhovec S, Bernik I, Markelj B. Explaining information seeking intentions: insights from a Slovenian social engineering awareness campaign. Computers & Security. 2023; 125:103038.
[26] Balogun NA, Abdulrahaman MD, Aka K. Exploring the prevalence of internet crimes among undergraduate students in a Nigerian university: a case study of the university of Ilorin. Nigerian Journal of Technology. 2024; 43(1):71-9.
[27] Childers G, Linsky CL, Payne B, Byers J, Baker D. K-12 educators' self-confidence in designing and implementing cybersecurity lessons. Computers and Education Open. 2023; 4:100119.
[28] Wusylko C, Xu Z, Dawson KM, Antonenko PD, Koh DH, Lee M, et al. Using a comic book to engage students in a cryptology and cybersecurity curriculum. Journal of Research on Technology in Education. 2024; 56(4):373-91.
[29] Kim SK, Jang ET, Park H, Park KW. Pwnable-sherpa: an interactive coaching system with a case study of pwnable challenges. Computers & Security. 2023; 125:103009.
[30] Purbo OW, Prasetyo P, Dimaz AP, Agung BP, Tubagus AN. Identifying large young hacker concentration in Indonesia. Journal of Internet Services and Information Security. 2024;14(1):52-63.
[31] Ortiz-garcés I, Govea J, Sánchez-viteri S, Villegas-ch W. CyberEduPlatform: an educational tool to improve cybersecurity through anomaly detection with

artificial intelligence. Peer Journal Computer Science. 2024; 10:1-33.
[32] Reddy B, Nagal A, Sood AK, Reddy SLR. Enhancing cyber security at scale with ML/AI frameworks. Network Security. 2023; 2023(5):83-91.
[33] Soon JNP, Chan RQ, Lee QH, Loke DE, Chun SLH, Yuen PK. User perceptions of artificial intelligence powered phishing attacks on facebook's resilient infrastructure. International Journal of Advances in Applied Sciences. 2024;13(4):878–86.
[34] Mishra N, Shivaji GB, Barekar SS, Dari SS, Dhabliya D, Patil M. Artificial intelligence and machine learning in healthcare cybersecurity of current applications and future directions. South Eastern European Journal of Public Health. 2024; 23(2):56-61.
[35] Padli P, Setiawan Y, Soniawan V, Mardela R. Developing robotic cricket batting test technology with camera sensor and grid system. International Journal of Interactive Mobile Technologies. 2023; 17(7): 58-68.
[36] Fisher D. Mathematics mobile blended learning development: student-oriented high order thinking skill learning. European Journal of Educational Research. 2022; 11(1):69-81.
[37] Zanke A, Weber T, Dornheim P, Engel M. Assessing information security culture: a mixed-methods approach to navigating challenges in international corporate IT departments. Computers & Security. 2024:103938.
[38] Alhadidi I, Nweiran A, Hilal G. The influence of cybercrime and legal awareness on the behavior of university of Jordan students. Heliyon. 2024; 10(12):1-16.
[39] Thron E, Faily S, Dogan H, Freer M. Human factors and cyber-security risks on the railway–the critical role played by signalling operations. Information & Computer Security. 2024; 32(2):236-63.
[40] Mohanty SN, Singh T, Goel R, Baral SK, Kumar R. A study on building awareness in cyber security for educational system in India using interpretive structural modellings. International Journal of System Assurance Engineering and Management. 2024; 15: 2518–28.
[41] Zhu Q, Luo X, Liu Y, Gan C, Wu Y, Yang LX. Impact of cybersecurity awareness on mobile malware propagation: a dynamical model. Computer Communications. 2024; 220:1-11.
[42] Samala AD, Howard NJ, Budiman RD, Hakiki M, Hidayah Y. What does an IMoART application look like? IMoART--an interactive mobile augmented reality application for support learning experiences in computer hardware. International Journal of Interactive Mobile Technologies. 2024; 18(13): 148:65.
[43] Taherdoost H. Towards an innovative model for cybersecurity awareness training. Information. 2024; 15(9):1-19.
[44] Hodhod R, Hardage H, Abbas S, Aldakheel EA. CyberHero: an adaptive serious game to promote cybersecurity awareness. Electronics. 2023; 12(17):1-18.
[45] Ortiz-garces I, Gutierrez R, Guerra D, Sanchez-viteri S, Villegas-ch W. Development of a platform for learning cybersecurity using capturing the flag competitions. Electronics. 2023; 12(7):1-15.
[46] Kim M, Jo D, Jeong J. Evaluation of mobile risk perception training system for improving the safety awareness of construction workers. Buildings. 2023; 13(12):1-14.

Dr. Fivia Eliza is an Associate Professor in the Electrical Engineering Education Study Program at the Faculty of Engineering, Padang State University. Her research interests include Technology Enhanced Learning, Instructional Design and Delivery, Philosophy of Vocational Education, Mobile Learning, E-Learning, Instructional Media, and Trainers.
Email: fivia_eliza@ft.unp.ac.id

Radinal Fadli is a Doctoral Candidate in Technology and Vocational Education, Universitas Negeri Yogyakarta, Sleman, Indonesia. Currently working as a lecturer and researcher at Universitas Muhammadiyah Muara Bungo, Bungo, Indonesia. His research interests include Digital Learning, Online Learning, Mobile Learning, Educational Media, Network Technology, and Cybersecurity.
Email: fadliradinal@gmail.com

Dr. Yayuk Hidayah is a Lecturer and Researcher in Social Sciences at Universitas Negeri Yogyakarta, Sleman, Yogyakarta, Indonesia. Her research interests include Educational Philosophy, Social Aspects and Learning Behaviors, Educational Psychology, Curriculum Innovation, Learning Evaluation and Learning Media,
Email: yayukhidayah@uny.ac.id

Prof. Herman Dwi Surjono is an expert in the field of Educational Media with extensive experience and impressive achievements. He was ranked 51st out of 100 leading open and distance education scientists in 2023. He was recognised as an Outstanding Lecturer in the Group of Professors in 2020. He is the dean of the Faculty of Engineering at Yogyakarta State University and has taught in education and engineering informatics for over 20 years. Apart from that, he dedicates his knowledge by providing training in the use of technology in education, helping to spread

knowledge and skills to the next generation and fellow professionals in this field.
Email: hermansurjono@uny.ac.id

Dr. Ratna Candra Sari is an Associate Professor, Researcher, and Financial Literacy Practitioner. He received his Doctoral degree from Gajah Mada University as a lecturer and researcher at the Faculty of Economics and Business, Yogyakarta State University. Dr. Ratna has made significant contributions to education and research in economics and finance. He received an Award from the Yogyakarta Association of Islamic Economic Experts in 2022. Apart from that, he dedicates himself as a speaker at various seminars, providing knowledge and insight regarding the digital economy and financial literacy to multiple audiences.
Email: ratna_candrasari@uny.ac.id

Appendix I

S. No.	Abbreviation	Description
1	4D	Define, Design, Develop, Disseminate
2	AI	Artificial Intelligence
3	CTF	Capture The Flag
4	DFD	Data Flow Diagram
5	ERD	Entity-Relationship Diagram
6	E-Money	Electronic Money
7	QRIS	Quick Response Code Indonesian Standard
8	SWD	System Work Design
9	WiFi	Wireless Fidelity