Evaluating and Boosting Cybersecurity Awareness With an AI-Integrated Mobile App

Meera Alalawi †
Information Systems and Security
College of IT
United Arab Emirates University
Al Ain, United Arab Emirates
700038186@uaeu.ac.ae

Nisha Thorakkattu Madathil†
Information Systems and Security
College of IT
United Arab Emirates University
Al Ain, United Arab Emirates
201990156@uaeu.ac.ae

Simon Kebede Darota
Information Systems and Security
College of IT
United Arab Emirates University
Al Ain, United Arab Emirates
201950317@uaeu.ac.ae

Winner Abula
Information Systems and Security
College of IT
United Arab Emirates University
Al Ain, United Arab Emirates
201950320@uaeu.ac.ae

Saed Alrabaee*
Information Systems and Security
College of IT
United Arab Emirates University
Al Ain, United Arab Emirates
salrabaee@uaeu.ac.ae

Suhib Bani Melhem
United Arab Emirates University
Al Ain University
Abu Dhabi, United Arab Emirates
suhibmelhem@gmail.com

***Abstract*—This innovative practice full paper describes cybersecurity Awareness With an AI-Integrated Mobile Application. In the current digital age, where technology and interactions are closely intertwined, the importance of cybersecurity awareness has escalated. It is essential for protecting individuals, organizations, and national security. This awareness enables people to make well-informed decisions and apply effective measures against cyberattacks. Human errors and behaviors often inadvertently lead to vulnerabilities, risking exposure to cyber threats. This paper focuses on developing an AI-enhanced mobile application tailored for diverse user groups: children under 14, teenagers between 14 and 18, adults over 18 (including university students, graduates, and the unemployed), and employees. The application aims to evaluate and offer extensive cybersecurity education content divided into three levels for each category, including lessons, videos, stories, scenarios, and exercises to enhance individual awareness levels. Additionally, it leverages AI to provide engaging cybersecurity responses, assess individuals, and support users with chatbot assistance. This strategy educates and empowers users, contributing to a more secure digital landscape.**

***Index Terms*—Cybersecurity, Cybersecurity Awareness, Artificial Intelligence, Mobile Application**

I. Introduction

IN the digital era, the landscape of education has experienced a transformational upheaval, altering the conventional paradigms of learning. The development of technology has not only widened the accessibility of knowledge but has also brought fresh techniques to education systems globally. This age, distinguished by fast technological innovations, necessitates an educational framework that is flexible, dynamic, and integrated with digital technologies. Modern education institutions are increasingly embracing digital platforms to support interactive and individualized learning experiences [1], [2]. The emphasis has switched from simple memorizing to fostering critical thinking and problem-solving abilities, preparing pupils for the challenges of the current world. Digital tools and resources, such as online courses, interactive applications, and virtual classrooms, have become vital components of modern education, allowing learners freedom and a wealth of learning options outside the conventional classroom walls [3]. The incorporation of technology in education not only enriches learning experiences but also educates students with vital digital literacy skills necessary for navigating the difficulties and possibilities of the digital age [4], [5].

The importance of cybersecurity education has reached new heights in today's quickly changing digital environment. As our dependence on digital platforms grows, cybersecurity plays a crucial role in securing sensitive information and defending against cyberattacks [6]–[8]. The increasing reliance on digital technology has heightened the susceptibility of people, corporations, and governments to cyber assaults. Given this understanding, the contemporary education system has a key function to fulfill [9]. The institution is aggressively integrating cybersecurity into its curriculum to reflect the increasing significance of digital security and data safeguarding in our daily lives [10]. By integrating these concepts, the school system is not only increasing knowledge about possible dangers like phishing, malware, and data breaches but also establishing a basis for secure digital behaviors among students. Moreover, with the increasing demand for cybersecurity experts, educational programs in this domain are creating

* Corresponding Author: Saed Alrabaee, salrabaee@uaeu.ac.ae

† These authors contributed equally to this work.

numerous career prospects [11]. This is in line with the main objective of equipping students for the future job market and promoting a sense of legal and ethical responsibility in digital behavior [12], [13].

The need for extensive cybersecurity understanding is currently more critical than ever. In the age of pervasive online contact, it is essential for every individual to possess the necessary skills to safeguard personal and sensitive data from emerging cyber threats [14]. Having this understanding is essential, not just for individual safety but also for ensuring strong corporate security. Modern businesses are always at risk of experiencing data breaches, which have the potential to cause significant financial losses and harm their brand. Hence, it is essential for firms to prioritize cybersecurity education in order to strengthen their defenses against such attacks. At a broader level, cybersecurity is crucial for safeguarding national security by defending against cyber warfare and espionage. Through the education of future cybersecurity professionals, we are safeguarding both our present digital infrastructure and strengthening our future defenses against the constantly changing landscape of cyber risks. Integrating cybersecurity education into mainstream learning is not just a passing educational fad, but a crucial and strategic action to guarantee a secure and robust digital future for everyone [15], [16].

In a nutshell, it is not only a trend but rather a must that cybersecurity education be included in the current educational system. It provides people with the information necessary to safeguard themselves and their businesses and contributes to the overarching objective of establishing a secure and resilient digital environment in today's world.

Here, we present our most recent advancement in the field of digital education: state-of-the-art mobile cybersecurity education software. This software, which was created with the needs of contemporary learners in mind, is a complete tool that will transform the way you study as well as a doorway to grasp cybersecurity ideas. It's designed to help you study more effectively, achieve better learning outcomes, and make complicated topics easier to comprehend. Our app is a valuable tool for anybody wishing to learn more about cybersecurity since it blends innovative teaching techniques with practical learning practices. Our software offers an interactive, captivating, and user-friendly platform for exploring and mastering the nuances of cybersecurity, regardless of your level of experience. Prepare yourself to set out on a life-changing educational adventure that will provide you with the tools you need to remain ahead in this quickly changing digital world.

II. Literature Review

Due to cyber threats' increasing complexity, AI in cybersecurity education is a fast-growing field in current literature. AI's pattern recognition capabilities are revolutionizing cybersecurity systems, particularly threat detection and response. AI-focused curricula are being added to schools to educate pupils about AI-driven security systems. Research shows that real-world AI tool implementations in education improve technical skills and knowledge of AI's ethical and social consequences in cybersecurity. AI automating mundane cybersecurity jobs indicates career changes and skill requirements. Scholarly debates often focus on AI-driven system malice and the need for robust ethical rules. This combination of AI and cybersecurity in education has great promise but requires careful thought and constant dialog among educators, technologists, and policymakers [1], [17]–[19].

Table I presents a comprehensive overview of recent games and mobile applications designed to enhance cybersecurity awareness, covering a range of target audiences and educational focuses. In 2021, "Cyber-Hero" was introduced specifically for high school students, focusing on educating them about human errors in cybersecurity, such as password creation. "Riskio," a 2020 tabletop card game, and "CybAR," an Augmented Reality mobile application launched the same year, target both employees with no technical background and university students. These games emphasize the understanding of cybersecurity attacks and defenses in an engaging learning environment.

The scope of these games extends to a general audience as well, with offerings like "CSRAG" (2019) and "SREG" (2018) that broadly cover security concepts, threats, and defenses. In a more specialized context, "CySecEscape 2.0," launched in 2021, serves as a virtual escape room experience, catering to employees of small and medium-sized enterprises with basic to advanced IT knowledge. This game encompasses various aspects of cybersecurity, from physical security to phishing and online banking. For younger users, "CyberKids" (2020) provides a playful platform to learn about cybersecurity, focusing on strong passwords and vulnerability identification, targeted at children aged 8 to 12 years. These diverse offerings highlight the increasing recognition of the importance of cybersecurity awareness across all age groups and professional backgrounds in the digital age.

On the other hand, a few studies have highlighted the potential of mobile applications in enhancing cybersecurity awareness. Authors in [27] introduced 'CyberAware,' a mobile app that uses the Theory of Planned Behavior (TPB) combined with context-based information, significantly boosting users' cybersecurity awareness and influencing their behaviors. Another study [28] focused on Malaysian secondary school students, developing the 'LetSecure' app to address gaps in cybersecurity knowledge by offering interactive learning tools and career guidance. Finally, authors in [29] developed an educational app targeting Arabic-speaking individuals in the MENA region, providing localized cybersecurity content and gamified learning to improve awareness. These studies underscore the importance of personalized, accessible cybersecurity education across different demographics.

Therefore, the gamification and mobile applications presented in Table I have shown significant promise in enhancing cybersecurity awareness across diverse demographics and settings. The positive outcomes observed in these studies underscore the effectiveness of integrating narrative and interactive elements into cybersecurity education, making it more

TABLE I: Recent Proposed Games and Mobile Applications to Increase Cybersecurity Awareness

Ref.	Game or Mobile App	Focus or Goal	Target Audience
[20]	Cyber-Hero	Educate students about human errors and how to be protected from cyberattacks by creating strong passwords.	High School Students
[21]	Riskio	A tabletop cards game to increase cyber security awareness, specifically on cyber security attacks and defences in an active learning environment	Employees with no technical background and university students
[22]	CSRAG	A card-based game that improves awareness of general security concepts, threats, and possible ways to identify potential threats in operation environment.	General Audience
[23]	SREG	Educates players about security requirements based on identified vulnerabilities and security attack scenarios	General Audience
[24]	CySecEscape 2.0	A virtual escape room to raise cybersecurity awareness including physical security, password hygiene, source code security, information disposal, securing sensitive digital data, identity theft and phishing, and online banking.	Small and medium-sized enterprises employees with basic IT knowledge and advanced IT players
[25]	CybAR	Increase Cybersecurity Awareness using an Augmented Reality mobile application that educates users about cybersecurity concepts and demonstrates the consequences of cybersecurity attacks.	General Audience with no technical background
[26]	CyberKids	A playful application that integrates and delivers basic educational content on cybersecurity, including games to increase awareness of strong passwords and identify vulnerabilities	Users aged 8 to 12 years
[27]	CyberAware	Provide users with both effective warnings and relevant cybersecurity information.	Android Audience
[28]	LetSecure	A beginner-friendly educational tool designed to enhance understanding of cybersecurity concepts and encourage interest in cybersecurity careers.	Secondary School Students
[29]	Beware of the Hacker	Enhancing cybersecurity awareness through multiple-choice questions, terms, and articles related to cybersecurity awareness.	Adult Arabic-speaking individuals in the MENA region

engaging and accessible to many users.

III. METHODOLOGY

A. *"AMNAK" Overview*

As technology advances, new vulnerabilities are discovered [1], [30], [31], and hackers continuously adapt their hacking techniques, individuals should stay updated with the latest best practices and be aware of the latest attacks to protect themselves and their sensitive data from cybercriminals. Therefore, this project focuses on equipping individuals with the needed cybersecurity awareness through a mobile application. The application will focus on evaluating and providing comprehensive cybersecurity education content to raise the level of cybersecurity awareness among individuals.

As presented in Figure 1, the mobile application is designed for four main categories: users under 14 (Elementary and middle school students), users between 14 and 18 (high school students), users above 18 (university students and graduates/unemployed), as well as employees. Each user in each category will be assigned to beginner, intermediate, or advanced levels based on their cybersecurity knowledge test results; however, the users will have the option to access higher levels within the same category. The beginners level will cover the basic non-technical introductory information to help users understand the fundamental concepts of cybersecurity awareness, users in the intermediate level will have access to a well-rounded learning experience with both non-technical and technical content, and the advanced level is tailored for users with prior cybersecurity knowledge; the material for this level is more specialized, offering a solid grounding in cybersecurity awareness.

The application content will include lessons, videos, quizzes, scenarios, games, stories, labs, daily news, roadmaps, security and privacy tips and recommendations that focus on the following domains: information security, application security, network security, could security, data security, computer/digital forensics, incident responses, end-user behaviors, etc. The tiered approach has been designed to cater to the unique learning pace of every user. It enables them to initiate the learning process from the foundation and gradually advance their knowledge or make quick progress if they already possess prior knowledge. The structured path ensures a continuous learning experience and helps develop essential cybersecurity awareness. The application includes quizzes and evaluation tests specified for each category to measure users' progress effectively. Further, the application features an AI chatbot powered by OpenAI to offer accurate and helpful responses to users related to cybersecurity and application content.

The application's cybersecurity content was expertly developed by team members specializing in cybersecurity. The material was drawn from various high-level, trusted organizations and academic sources to ensure its accuracy and relevance. Complex cybersecurity concepts are presented in a manner that is easily understood by different age groups. This approach ensures that users of all backgrounds can effectively engage with and benefit from the educational material provided in the application.

B. *"AMNAK"- System Design*

1) *Front-End Development*

a) *React Native Framework*

The front-end of the AMNAK mobile application is developed using the React Native framework [32], a popular open-source framework for building cross-platform mobile applications. React Native allows for the creation of a seamless and consistent user experience across both iOS and Android platforms. Leveraging the power of React, developers can build reusable UI components, enabling efficient development and maintenance of the application.

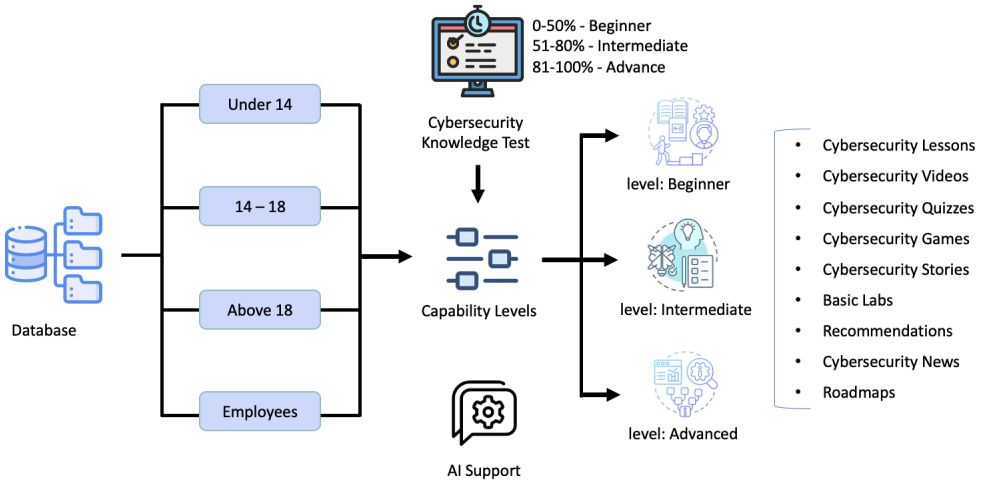

Fig. 1: ”AMNAK” Overview Structure

*b) **User Interface (UI) Design***

The user interface design of AMNAK is carefully crafted to provide an intuitive and user-friendly experience. The design principles prioritize simplicity, ensuring that users can easily navigate through the app and access its features. A responsive layout accommodates various screen sizes and orientations, enhancing the app's adaptability on a wide range of mobile devices.

*c) **Integration with Firebase Authentication***

To ensure secure user authentication, AMNAK integrates with Firebase Authentication. This allows users to create accounts, log in securely, and reset passwords if needed. Firebase Authentication provides a robust and scalable solution for identity management, enhancing the overall security of the application.

*2) **Back-End Development***

*a) **Firebase Cloud Firestore for Text-Based Data***

AMNAK leverages Firebase Cloud Firestore for storing and managing text-based data. Cloud Firestore is a NoSQL document database that enables real-time synchronization of data between the front-end and back-end. This ensures that users have up-to-date information and allows for efficient querying of data. The use of Firestore also provides scalability, making it well-suited for the dynamic nature of a mobile application [33].

*b) **Firebase Cloud Storage for Image and Video Storage***

For handling multimedia content such as images and videos, AMNAK utilizes Firebase Cloud Storage. This cloud-based storage solution allows the seamless upload, download, and management of media files. The integration with Cloud Storage ensures reliable and scalable storage for the diverse range of media content that the application may handle. It also facilitates easy retrieval and display of multimedia content within the app.

IV. Implementation and Results

The application interface is designed to offer a user-friendly experience. It starts with a login page that includes fields for email and password, along with links for creating a new account and password retrieval. The account registration module is comprehensive, gathering information such as username, email, password (with confirmation), date of birth, and occupation to ensure a detailed user profile. Based on the registration information, the users will be categorized into four categories: users under 14, users between 14 and 18, users above 18, and employees. Once the user logs in, a beginning evaluation quiz will be presented to gauge the user's cybersecurity knowledge as presented in Figure 2; this interactive test features multiple-choice random questions designed to assess users' understanding of cybersecurity. Based on the users' results, they will be assigned to beginners, intermediates, and advanced levels. The quiz interface is intuitive, with straightforward navigation buttons to move between questions and submit answers.

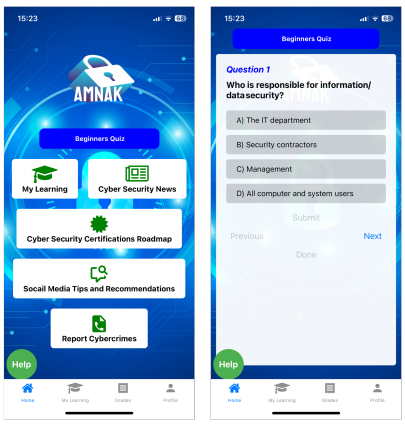

Fig. 2: Beginning Test

A. *My learning*

The ”AMNAK” mobile application's homepage offers universal access to its various features, while the ”My Learning”

section is customized to fit different user groups, providing age and role-specific educational content. Younger school students can explore interactive materials such as videos, stories, and exercises organized into beginner, intermediate, and advanced levels, as shown in Figure 3. University students, graduates, or unemployed individuals above 18 are offered structured cybersecurity lessons across the same skill levels to enhance their cybersecurity awareness. The employed user's category receives specialized content focusing on cybersecurity in the workplace, addressing the critical need for professional and personal cybersecurity awareness. This personalized approach within the App ensures that each user receives an educational experience that aligns with their developmental stage or professional requirements.

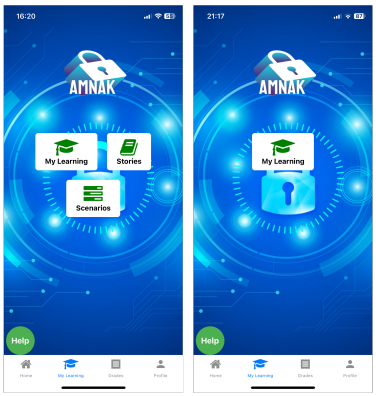

Fig. 3: Users under 18 Learning page (left) and Users above 18 Learning page (Right)

*1) **Users Aged Under 18***

*a) **Users under 14 (School Students)***

School students under the age of 14 will be offered content on cybersecurity awareness, concepts, and best practices, which is stratified into beginner, intermediate, and advanced levels. This content is delivered through interactive and captivating formats to engage students and enhance their understanding of cybersecurity.

*b) **Users between 14 and 18 (High School Students)***

The App provides advanced cybersecurity content for high school students aged between 14 and 18 years old. This content is an extension of the material provided to the under-14 category age group, but it is tailored to deepen their knowledge of cybersecurity concepts. The App engages students through interactive content, including thought-provoking videos and challenging scenarios designed to provoke critical thinking and reflection on cybersecurity best practices. The App also includes comprehensive quizzes, exercises to identify secure online behaviours and relatable stories that weave cybersecurity concepts together. Although the foundational topics are similar to those aimed at younger users, the approach is elevated to match high school students' advanced understanding and cognitive abilities.

*c) **Content and Activities***

The application features animated videos designed to educate users under 18 about cybersecurity. These videos are narrated in an engaging and appropriate tone for a younger audience, making the learning process enjoyable and informative. Tailored to match the viewers' age and comprehension abilities, the videos cover essential internet concepts in a clear and accessible manner. After watching the videos, users are encouraged to take a quiz that tests their understanding of the content. This interactive quiz assesses their grasp of the material and reinforces the information presented in the video, significantly enhancing the overall learning experience, as shown in Figure 4.

The application includes interactive stories that enhance cybersecurity awareness among users under 18. These stories are crafted to be relatable and engaging, featuring scenarios the young audience might encounter in daily digital interactions. For example, as illustrated in Figure 4, the story "Ahmed and Ali's Social Media Adventures" illustrates the pressures of social media sharing and the importance of making thoughtful choices online. After reading the stories, users are prompted to reflect on the lessons learned by writing down key takeaways. This exercise encourages users to internalize safe online behaviours and understand the consequences of their digital actions.

In addition to videos and stories, the application presents interactive scenarios that simulate real-world challenges young users might face online. These scenarios are designed to test users' ability to apply their cybersecurity knowledge in practical situations. For instance, as shown in Figure 4, users decide how to share photos online and safely recognise and report inappropriate content. Each scenario provides multiple-choice responses, and upon selection, the app explains why the chosen option is correct or incorrect. This section enhances decision-making skills regarding internet safety and provides immediate feedback, helping users learn the appropriate actions to take in various digital circumstances.

*2) **Users Aged Above 18***

*a) **University Students, Graduates, Unemployed***

The application provides structured content of cybersecurity lessons tailored for individuals above 18, including university students, graduates, or the unemployed. The content is systematically organized into beginners, intermediates, and advanced levels to cater to learners at different stages of their cybersecurity education. Starting with the basics, users are introduced to the fundamental concepts and principles of cybersecurity, progressing through a series of topics that grow in complexity. As learners advance, they delve into intricate subjects such as malware, the nuances of social engineering attacks, and strategies to counteract various cyber threats. Each lesson culminates in an interactive quiz reinforcing the content learned and evaluating the user's understanding, as represented in Figure 5. Quiz results are immediately provided, giving valuable feedback that allows users to gauge their competency in each topic and identify areas needing additional focus, thus facilitating a complete and effective educational experience in cybersecurity.

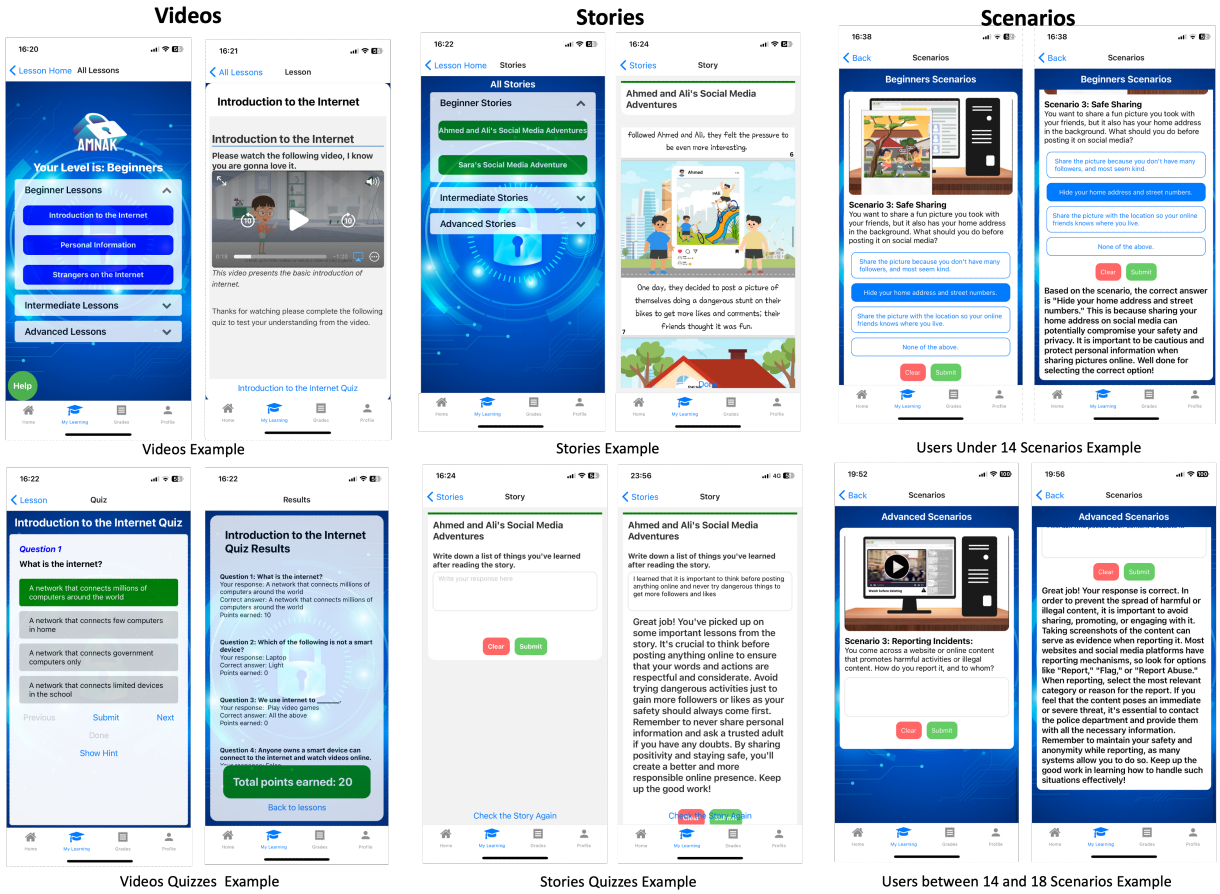

Fig. 4: Users Under 18 content example

*b) **Employees***

The application offers cybersecurity lessons specifically designed for employees, targeting the critical awareness needed to protect sensitive data in today's organizational landscape. These lessons cover contemporary issues such as AI-driven scams, providing employees with the knowledge to identify and mitigate such threats. Upon completing a lesson, employees are presented with multiple-choice questions that evaluate their understanding of the subject matter, as shown in the example in Figure 5. The quiz results provide immediate feedback, allowing for a clear assessment of their learning progress and ensuring they have grasped essential cybersecurity concepts critical for protecting their organization's digital assets.

*3) **Evaluation Tests and Grades***

Users across all categories—under 14, ages 14 to 18, above 18, and employees—can access tailored evaluation tests within the application, designed to gauge their understanding of cybersecurity. These tests allow for multiple attempts and can be taken anytime, providing flexibility and continuous learning opportunities. Results from each attempt are recorded and displayed on the user's grades page, ensuring a clear view of progress and areas for improvement. The App generates 15 random multiple-choice questions for each evaluation from a comprehensive question bank that spans the content specific to each user category, ensuring a broad assessment.

B. Home Page Features

The "AMNAK" application's home page presents a range of features that cater to users across all categories—under 14, 14 to 18, above 18, and employees. Alongside the "My Learning" component, which delivers age and role-specific content, the App provides universally accessible tools. These include "Cyber Security News," a "Cyber Security Certifications Roadmap," "Social Media Tips and Recommendations" related to privacy and security, and "Report Cybercrimes," where users will be directed to concerned authorities. Additionally, a "Games" section offers educational games reinforcing cybersecurity concepts. This layout ensures that users from any category can easily navigate and utilize the resources tailored to enhance their cybersecurity knowledge and skills.

*1) **Security News***

The application features a dedicated section for recent cybersecurity news, keeping users informed about the latest developments and threats in the field of cybersecurity. This section not only highlights important news events but also directs users to the original sources for in-depth reading. This functionality emphasizes the App's role as an educational tool, ensuring that users are not only learning about cybersecurity

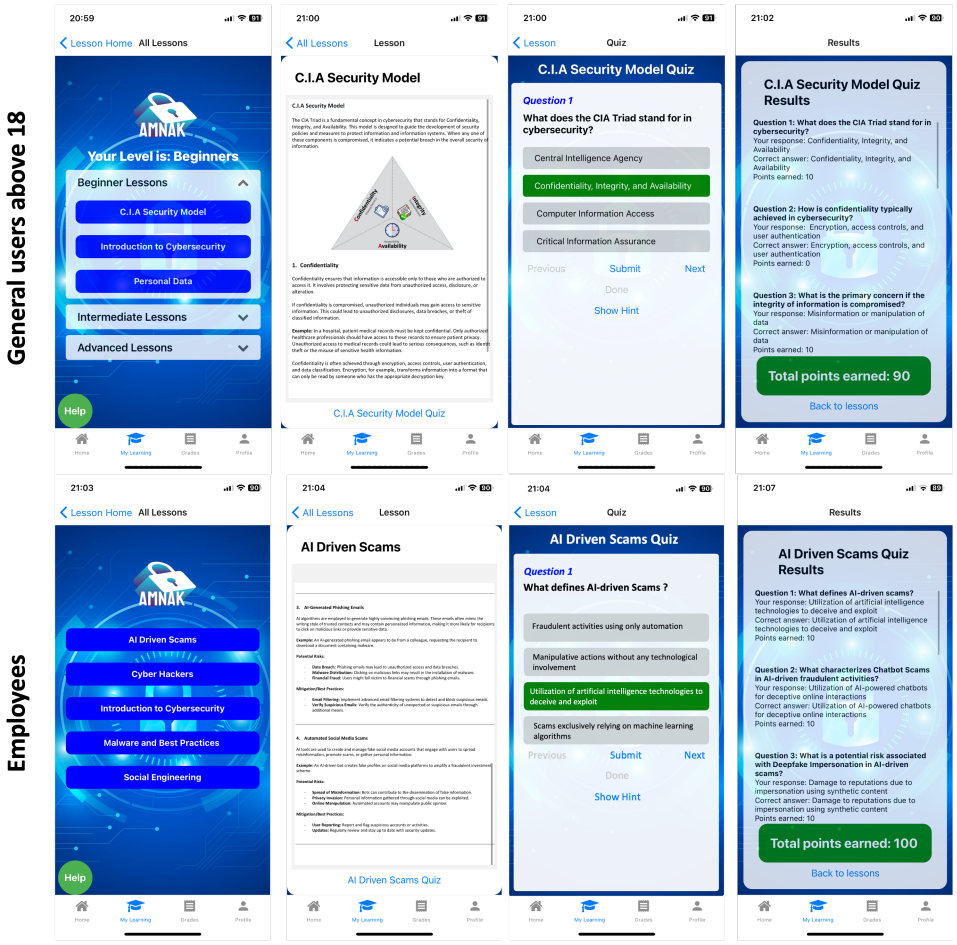

Fig. 5: above 18 content example

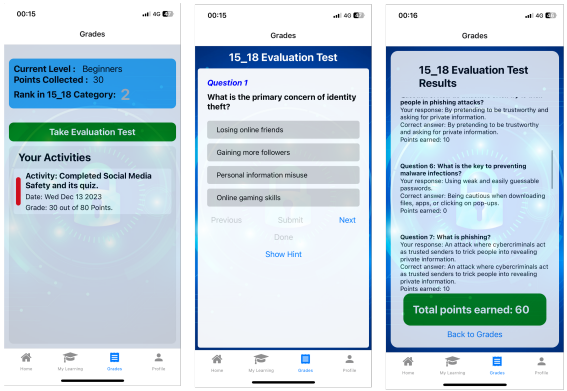

Fig. 6: Evaluation Test and Grades Page

practices but are also aware of real-world applications and incidents.

*2) **Report Cybercrimes***

The ”AMNAK” application has a helpful feature for users who want to report cybercrimes but are unsure of the appropriate channel. The App provides direct links to the official websites of the relevant authorities, enabling users to communicate their cybersecurity concerns promptly and securely to the proper channels.

*3) **Security Certifications Roadmap***

The application presents a systematically organized and updated security certification roadmap inspired by Paul Jerimy’s framework [34] tailored for IT and cybersecurity professionals. It categorizes certifications according to experience levels, directing users towards the most appropriate credentials for their career goals. The roadmap prioritizes obtaining relevant certifications over numerous others, aligning with the National Initiative for Cybersecurity Careers and Studies (NICCS) standards to offer a defined path for professional growth and advancement in the industry.

*4) **Social Media Tips and Recommendations***

The application furnishes users with essential security and privacy tips for social media, complemented by step-by-step instructions to make the process easier to navigate. This feature is designed to help users enhance their digital safety and privacy on various platforms by walking them through recommended security measures.

C. AI Assistant

In the application, GPT Turbo 3.5 serves both as a virtual service assistant and as a mechanism for delivering feedback and grades on user activities. It utilizes prepared prompts and dynamically generates responses to user inquiries or details

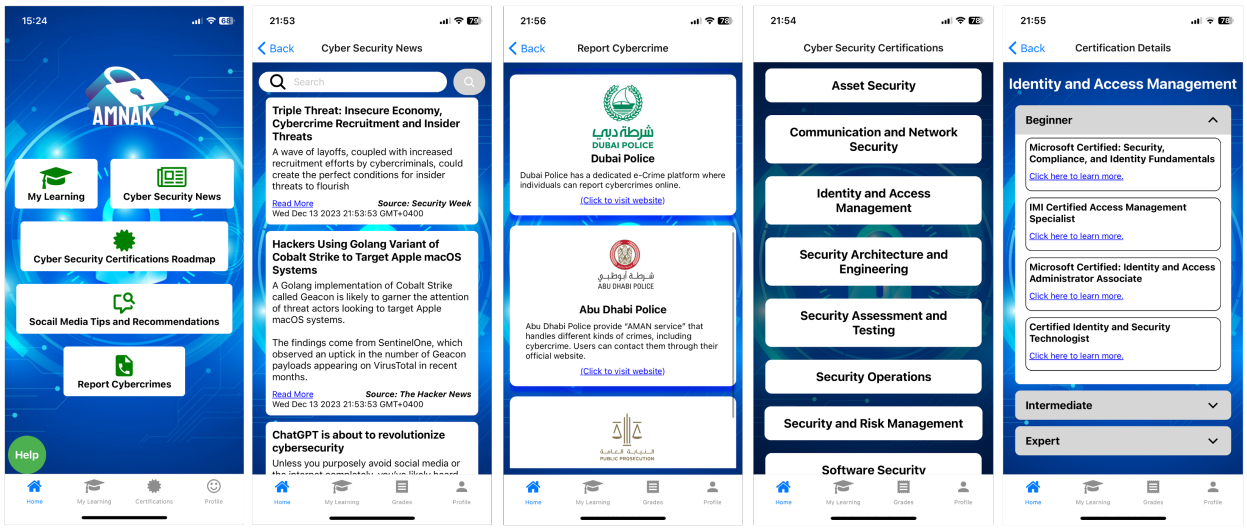

Fig. 7: Home Page Features

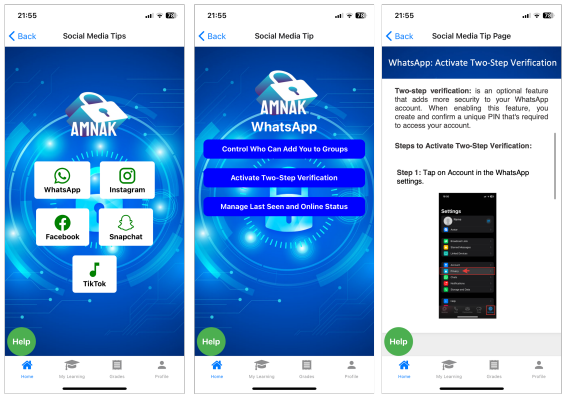

Fig. 8: Social Media Tips and Recommendations Page

about completed exercises, which are processed through the GPT API. GPT Turbo 3.5 leverages its advanced NLP capabilities to understand the queries and provide apt responses. As a virtual assistant, it helps users by answering questions and offering necessary information. In terms of exercises, the API assesses users' submissions and provides feedback, integrating intelligent automation into the app's engagement and support functions. This dual role of GPT Turbo 3.5 significantly enriches the user experience by facilitating personalized and contextually appropriate interactions within the application. Figure 9 presents a response to "What is malware?" from the Help Assistant in the app, and another example is the responses in the activities provided to users, such as Figure 4

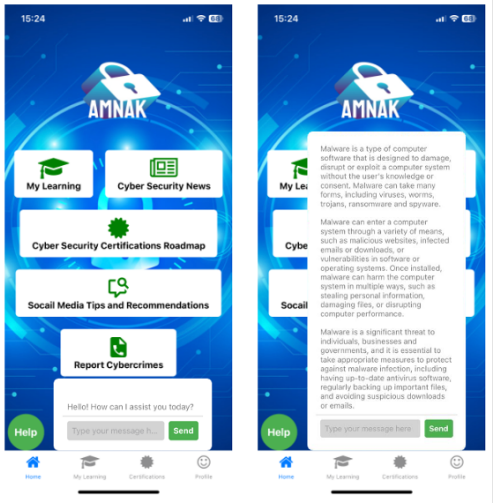

Fig. 9: GPT-API Integration

V. Conclusion

In conclusion, this paper presents the development of an AI-enhanced mobile application designed to elevate cybersecurity awareness across diverse user groups. By offering tailored educational content divided into beginner, intermediate, and advanced levels, the application provides a comprehensive learning experience that caters to different age groups and knowledge levels. Leveraging AI, the app delivers engaging content and offers real-time assessments and personalized support, empowering users to navigate the digital landscape securely. This approach underscores the critical role of education in mitigating cyber threats and emphasizes the importance of accessible, adaptable tools in fostering a safer online environment. Despite its potential, the application has certain limitations that need to be addressed. Currently, the app is developed only in English, which may limit its accessibility to non-English speakers. Additionally, the dynamic nature of cybersecurity means that the content requires constant updates to address the latest cyber threats and trends effectively. Without regular updates, the material could quickly become outdated, diminishing the application's relevance and effectiveness over time. In the future, the focus will be on broader empirical evaluations involving a larger and more diverse group of users to better understand the application's impact. Continuous content updates will be prioritized to ensure that the educational material remains current with

emerging cybersecurity challenges. Furthermore, efforts will be made to expand the application's reach and accessibility, including the development of multilingual support to cater to a global audience.

ACKNOWLEDGMENT

We are grateful to the anonymous reviewers for their comments and suggestions. This work is supported by AUA-UAEU Joint Research Grant number 12R170.

REFERENCES

[1] S. Grover, B. Broll, and D. Babb, "Cybersecurity education in the age of ai: Integrating ai learning into cybersecurity high school curricula," in *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1*, 2023, pp. 980–986.

[2] N. T. Madathil, W. Abula, S. Alaboolan, M. Almadhaani, and S. Alrabaee, "Pess: Progress enhancing student support," in *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*. IEEE, 2023, pp. 1–6.

[3] G. A. Garrett, *Cybersecurity in the Digital Age: Tools, Techniques, & Best Practices*. Aspen Publishers, 2018.

[4] N. T. Madathil, S. Alrabaee, M. Al-kfairy, R. Damseh, and A. N. Belkacem, "Ai in education: Improving quality for both centralized and decentralized frameworks," in *2023 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2023, pp. 1–6.

[5] S. Abdelhamid, T. Mallari, and M. Aly, "Cybersecurity awareness, education, and workplace training using socially enabled intelligent chatbots," in *The Learning Ideas Conference*. Springer, 2023, pp. 3–16.

[6] M. Bada and J. R. Nurse, "Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (smes)," *Information & Computer Security*, vol. 27, no. 3, pp. 393–410, 2019.

[7] K. Michael, R. Abbas, and G. Roussos, "Ai in cybersecurity: The paradox," *IEEE Transactions on Technology and Society*, vol. 4, no. 2, pp. 104–109, 2023.

[8] N. Sridhar, L. Yang, J. Joshi, and V. Piotrowski, "Cybersecurity education in the age of artificial intelligence," in *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*, 2021, pp. 1365–1365.

[9] L. Al Kaabi, W. Al Ketbi, A. Al Khoori, M. Al Shamsi, and S. Alrabaee, "Safe: Cryptographic algorithms and security principles gamification," in *2022 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2022, pp. 1169–1178.

[10] N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi, and F. Khalid, "The importance of cybersecurity education in school," *International Journal of Information and Education Technology*, vol. 10, no. 5, pp. 378–382, 2020.

[11] D. Valle-Cruz, J. I. Criado, R. Sandoval-Almazán, and E. A. Ruvalcaba-Gomez, "Assessing the public policy-cycle framework in the age of artificial intelligence: From agenda-setting to policy evaluation," *Government Information Quarterly*, vol. 37, no. 4, p. 101509, 2020.

[12] A. McGettrick, "Toward effective cybersecurity education," *IEEE Security & Privacy*, vol. 11, no. 6, pp. 66–68, 2013.

[13] I. Corradini and E. Nardelli, "Developing digital awareness at school: a fundamental step for cybersecurity education," in *Advances in Human Factors in Cybersecurity: AHFE 2020 Virtual Conference on Human Factors in Cybersecurity, July 16–20, 2020, USA*. Springer, 2020, pp. 102–110.

[14] E. C. Cheng and T. Wang, "Institutional strategies for cybersecurity in higher education institutions," *Information*, vol. 13, no. 4, p. 192, 2022.

[15] R. Trifonov, O. Nakov, S. Manolov, G. Tsochev, and G. Pavlova, "Possibilities for improving the quality of cyber security education through application of artificial intelligence methods," in *2020 International Conference Automatics and Informatics (ICAI)*. IEEE, 2020, pp. 1–4.

[16] R. Hodhod, S. Wang, and S. Khan, "Cybersecurity curriculum development using ai and decision support expert system," *International Journal of Computer Theory and Engineering*, vol. 10, no. 4, p. 111, 2018.

[17] M. Schmitt, "Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (ai)-enabled malware and intrusion detection," *Journal of Industrial Information Integration*, vol. 36, p. 100520, 2023.

[18] S. Dilek, H. Çakır, and M. Aydın, "Applications of artificial intelligence techniques to combating cyber crimes: A review," *arXiv preprint arXiv:1502.03552*, 2015.

[19] A. Rai, A. Jain, and A. S. Chauhan, "Fortifying the smart world: An in-depth look at security measures for iot devices," in *2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET)*. IEEE, 2023, pp. 619–624.

[20] H. Qusa and J. Tarazi, "Cyber-hero: A gamification framework for cyber security awareness for high schools students," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2021, pp. 0677–0682.

[21] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A serious game for cyber security awareness and education," *Computers & Security*, vol. 95, p. 101827, 2020.

[22] A. Yasin, L. Liu, T. Li, R. Fatima, and W. Jianmin, "Improving software security awareness using a serious game," *IET Software*, vol. 13, no. 2, pp. 159–169, 2019.

[23] A. Yasin, L. Liu, T. Li, J. Wang, and D. Zowghi, "Design and preliminary evaluation of a cyber security requirements education game (sreg)," *Information and Software Technology*, vol. 95, pp. 179–200, 2018.

[24] E. Löffler, B. Schneider, T. Zanwar, and P. M. Asprion, "Cysecescape 2.0—a virtual escape room to raise cybersecurity awareness," *International Journal of Serious Games*, vol. 8, no. 1, pp. 59–70, 2021.

[25] H. Alqahtani and M. Kavakli-Thorne, "Design and evaluation of an augmented reality game for cybersecurity awareness (cybar)," *Information*, vol. 11, no. 2, p. 121, 2020.

[26] J. Pérez, R. Torres, and S. Von Brand, "Cyberkids: video game for raising cyber security awareness in children," in *2020 39th International Conference of the Chilean Computer Science Society (SCCC)*. IEEE, 2020, pp. 1–8.

[27] V. Lombardi, S. Ortiz, J. Phifer, T. Cerny, and D. Shin, "Behavior control-based approach to influencing user's cybersecurity actions using mobile news app," in *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, ser. SAC '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 912–915. [Online]. Available: https://doi.org/10.1145/3412841.3442103

[28] A. M. Jafri, Z. Zulkifli *et al.*, "Cybersecurity awareness mobile apps for secondary school students: Letsecure," *Journal of Information Systems and Digital Technologies*, vol. 3, no. 2, pp. 94–108, 2021.

[29] H. M. Jawad and S. Tout, "Introducing a mobile app to increase cybersecurity awareness in mena," in *2020 3rd International Conference on Signal Processing and Information Security (ICSPIS)*. IEEE, 2020, pp. 1–4.

[30] J. Wei-Kocsis, M. Sabounchi, B. Yang, and T. Zhang, "Cybersecurity education in the age of artificial intelligence: A novel proactive and collaborative learning paradigm," in *2022 IEEE Frontiers in Education Conference (FIE)*. IEEE, 2022, pp. 1–5.

[31] H. Zare, "Hands-on artificial intelligence and cybersecurity education in high schools," Ph.D. dissertation, 2019.

[32] "React navigation," https://reactnavigation.org/, Accessed 2023.

[33] "Firebase," https://firebase.google.com/, Accessed 2023.

[34] P. Jerimy, "Security certification roadmap," https://pauljerimy.com/security-certification-roadmap/, Accessed 2023.