IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 August 2024, accepted 2 October 2024, date of publication 14 October 2024, date of current version 21 January 2025.

Digital Object Identifier 10.1109/ACCESS.2024.3479921

RESEARCH ARTICLE

Using Peer-Learning and Game-Based Instruction for Achieving Long-Lasting Knowledge of Cybersecurity in Primary Schools

MAJA VIDENOVIK[1], VLADIMIR TRAJKOVIK[2], TONE VOLD[3], LINDA VIBEKE KIØNIG[3], ANA MADEVSKA BOGDANOVA[2], AND SONJA FILIPOSKA[2]

[1]Center for Innovations and Digital Education Dig-Ed, Skopje, North Macedonia
[2]Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University in Skopje, 1000 Skopje, North Macedonia
[3]Department of Business Administration and Organizational Studies, Inland Norway University of Applied Sciences, 2318 Hamar, Norway

Corresponding author: Tone Vold (tone.vold@inn.no)

This work involved human subjects or animals in its research. The authors confirm that all human/animal subject research procedures and protocols are exempt from review board approval.

ABSTRACT As the world becomes increasingly dependent on technology, cybersecurity education has become more important than ever before. However, teaching cybersecurity to primary school students faces several challenges, including limited resources, lack of specialized teachers, and age-appropriate content. In this paper, we propose a new and innovative approach for teaching cybersecurity to primary school students, which addresses these challenges. The proposed approach, implemented with 339 students in five primary schools in North Macedonia, combines peer learning and a game-based approach to develop students' communication, collaboration, and critical thinking skills, and create engaging learning environments. Upper-grade students deliver lectures and create educational games for their lower-grade peers, fostering learning communities where students share their knowledge and experiences, and learn from one another's diverse perspectives. The game-based approach is used to create interactive and engaging learning environments where students design or play games to develop their critical thinking skills and empower their cybersecurity knowledge. Initial evaluation results after one year of implementing this cybersecurity learning concept, carried out with 124 students from three participating schools, indicate that students exposed to peer learning and a game-based approach could retain their knowledge, with their knowledge levels outperforming those of students who received traditional classroom instruction. Moreover, students have positive attitudes toward implemented approach and believe that it has effectively enhanced their communication, collaboration, and critical thinking skills while creating exciting and engaging learning environments. These findings suggest that this new and innovative approach has the potential to effectively teach cybersecurity to primary school students, fostering long-lasting knowledge and creating engaging learning environments. Its implementation can be easily adopted in different educational contents and surroundings.

INDEX TERMS Cybersecurity education, engaging learning environments, game-based approach, long-lasting knowledge, peer learning.

I. INTRODUCTION

The significance of cybersecurity education is evident. Studies reveal a shortage of cybersecurity professionals, highlighting the need for improvements in cybersecurity education [1], [2], [3]. These improvements should be implemented at all levels of education, starting with the basics of good digital behaviour in primary education. Primary schools can play a crucial role in teaching young students about cybersecurity and developing positive digital habits

The associate editor coordinating the review of this manuscript and approving it for publication was Utku Kose.

from an early age [4]. This education can cover topics such as internet safety, avoiding online scams, protecting personal information, and responsible digital citizenship. By educating students about these concepts at a young age, they will be better equipped to handle the challenges of the online world as they grow older. It can also create a culture of cybersecurity awareness and potentially identify young talent in the field for the future workforce. However, primary schools' cybersecurity education is currently limited. Many barriers prevent effective cybersecurity education in formal classroom environments, such as a shortage of qualified teachers and a lack of educational resources [5], [6]. Some initiatives such as ''Safer Internet Day'' (https://www.saferinternetday.org/) and ''Internet Matters'' (https://www.internetmatters.org/) provide educational resources to support primary school cybersecurity education, but a more systematic approach is needed.

The cybersecurity education varies globally, with sometimes notable differences between different countries [7]. For example, USA cybersecurity programs emphasize practical skills and hands-on experience while European programs often blend cybersecurity with broader computer science education. Both regions invest in government-supported initiatives to enhance cybersecurity education and workforce development [8].

Cybersecurity education for primary school students poses many challenges, such as limited resources, lack of specialized teachers, constantly evolving technology, limited access to technology, limited parent and community engagement, limited understanding of the concept, and providing age-appropriate content [9], [10], [11], [12], [13]. Various teaching approaches have been implemented to tackle these challenges, mainly focused on establishing an interactive and engaging learning environment.

One such approach is game-based learning, which delivers educational content through games and interactive activities. This approach has proven to effectively improve student interest, engagement, and learning outcomes [14], [15], [16]. It provides challenging, motivating and stimulating learning environments, fostering students' critical thinking and problem-solving skills [17]. Considering the digital culture of today's students, who tend to have shorter attention spans and prefer to explore and discover, game-based learning can effectively engage students in the learning process [18]. It also promotes active and self-directed learning, enabling students to progress at their own pace, including secure areas and genuine educational settings [19], [20]. Furthermore, it can benefit students requiring more time or repetition to understand the material thoroughly. Game-based learning can be highly personalized and adapted to different learning styles and individual needs, engaging students in self-assessment [21]. Games can also provide immediate feedback, allowing students to adjust their learning approach and learn from their mistakes, supporting individualized progress [22].

However, designing an educational game is a challenging task that requires considering various factors such as entertainment, education, and difficulty level based on student performance and providing immediate feedback [23], [24]. While designing educational games can be complex and time-consuming, the benefits are clear. Game-based learning has the potential to transform the traditional classroom, making learning more engaging, interactive, and effective. Despite its benefits, it should not be used as the sole instruction method but in conjunction with other teaching methods to create a well-rounded and comprehensive learning experience.

Another approach to establishing an interactive and engaging environment is peer learning, where students teach and support each other in learning, fostering cooperation and self-regulated learning. Peer learning refers to the students' activities where they can teach and support each other, promoting knowledge sharing and teamwork. This collaborative approach values cooperation over competition and encourages students to work together towards common learning goals [25]. In the last decade, many researchers have confirmed the positive impact of peer learning on students' learning and academic achievement [26]. At the same time, peer learning activities can enhance students' critical thinking skills, help them retain information better, and improve their overall academic performance [27].

Peer learning can increase student motivation, engagement, and confidence in their abilities and knowledge [28], [29], [30]. However, it also requires effective facilitation and guidance from the teacher. Through peer learning activities, students can engage in discussions, provide feedback, and share their experiences and perspectives, which can help deepen their understanding of the material [31], [32]. Furthermore, peer learning can promote the development of essential social and emotional skills, such as communication, leadership, and empathy, which are essential for success both in and outside the classroom [33].

Game-based learning and peer learning can be a good combination for addressing the challenges of cybersecurity education. They promote engaging, interactive, and dynamic learning, foster communication and collaboration, and make learning more enjoyable for students. In addition, these approaches address the challenges faced by the effective integration of cybersecurity education in primary schools.

Games can be used to present cybersecurity concepts in a more accessible and interactive manner, making it easier for students to comprehend complex ideas and retain the information. Facing realistic situations, students can develop a deeper understanding of online safety problems and learn how to behave online. The peer learning approach can encourage students to work together, share their knowledge and experiences, and learn from each other's strengths and weaknesses. Students can develop their communication and collaboration skills by working in groups and learning how to approach cybersecurity challenges from multiple perspectives. By incorporating these approaches into cybersecurity

education, students can develop the knowledge and skills they need to protect themselves and others while they are online.

The main goal of this paper is to propose a new and innovative approach for teaching cybersecurity in primary schools, combining the use of peer learning and a game-based approach. The effectiveness of this methodological approach was evaluated based on students' attitudes toward its implementation, particularly in relation to the skills development and the creation of engaging learning environments. Additionally, students' knowledge of the learned cybersecurity topic was evaluated after one year to determine whether implementing this approach helps to promote long-lasting knowledge. The research questions investigated in this paper are:

- Can this methodological approach (combination of peer learning and game-based approach) be used to develop students' communication, collaboration and critical thinking skills and create interesting and engaging learning environments for learning cybersecurity topics?
- Are there any gender differences when implementing peer learning and a game-based approach for cybersecurity topics?
- Is this combination of peer learning and game-based approach enabling students to acquire long-lasting knowledge in cybersecurity topics?

The proposed methodology for using a game-based approach and peer learning during cybersecurity education is described in the next section. Then, Section III presents the results from the implementation process, and a discussion about these results is elaborated in Section IV. Finally, Section V concludes the paper.

II. METHODOLOGY

This paper outlines a new approach to teaching cybersecurity in primary schools that combines peer learning and game-based approaches. The goal is to make learning about cybersecurity more engaging and interactive for students, especially teenagers, who may not be receptive to traditional teaching methods. This approach leads to developing students' communication and collaboration skills, and critical thinking and problem-solving skills concerning cybersecurity issues. The method uses peer learning to create a community of learners and game-based activities to encourage active participation and engagement.

Figure 1 illustrates the proposed methodological approach for teaching cybersecurity in primary schools, combining peer learning and game-based activities to enhance student engagement and understanding. The general idea is to utilize the skills and knowledge of upper-grade students to educate lower-grade students, creating a community of learners who actively participate in and contribute to the learning process. The approach involves several interconnected steps, each aimed at developing critical thinking, communication, collaboration, and problem-solving skills related to cybersecurity.

Upper-grade students' activities include:

(U1) Upper-grade students begin by searching for information on cybersecurity and misinformation. They analyze and evaluate this information and draw conclusions. These activities develop their critical thinking and analytical skills. As a result, they prepare workshops for lower-grade students.

(U2) Using the prepared materials, upper-grade students deliver workshops to lower-grade students. This step involves peer learning, open discussions, communication, and collaboration. In this way, they transfer their knowledge and skills to the lower-grade students, who participate in the workshops and provide feedback.

(U3) After conducting the workshops, upper-grade students design interactive games in Scratch, focusing on the most challenging cybersecurity issues identified during the workshops. This process helps them reinforce their knowledge and skills by creating engaging educational tools.

(U4) Finally, upper-grade students refine the games based on feedback from lower-grade students. They then create short educational videos using these games. Using this approach, they produce high-quality educational resources that can be used in various educational contexts.

Lower-grade students' activities include:

(L1) Lower-grade students participate in the workshops conducted by upper-grade students. They engage in discussions, learning through peer interaction and collaboration. In this way, they increase their understanding of cybersecurity and contribute feedback to help improve the educational materials.

(L2) Lower-grade students play interactive games designed by upper-grade students. This step emphasizes learning through play, critical thinking, and communication. In addition, they provide feedback on the games created by upper grade students, helping them to refine and improve the games further.

Teachers introduce peer and game-based learning methodology to students and monitor the entire process. During the process they focus on developing different skills among the students:

Focus on developing critical thinking skills: The proposed methodology emphasizes developing critical thinking skills. Students analyze information, make conclusions, and engage in discussions that challenge their understanding and reasoning.

Focus on peer learning: The approach heavily relies on peer learning, where students learn from each other. This method fosters a sense of community and collaboration, encouraging students to share knowledge and support one another.

Focus on game-based approach: The use of game-based learning is a key component of this methodology. Designing and playing games makes learning about cybersecurity engaging and interactive, helping students retain information more effectively.

The final output includes a collection of open educational resources, such as teaching materials, Scratch-based games, and educational videos. These resources are shared online and can be used by teachers, students, and other interested

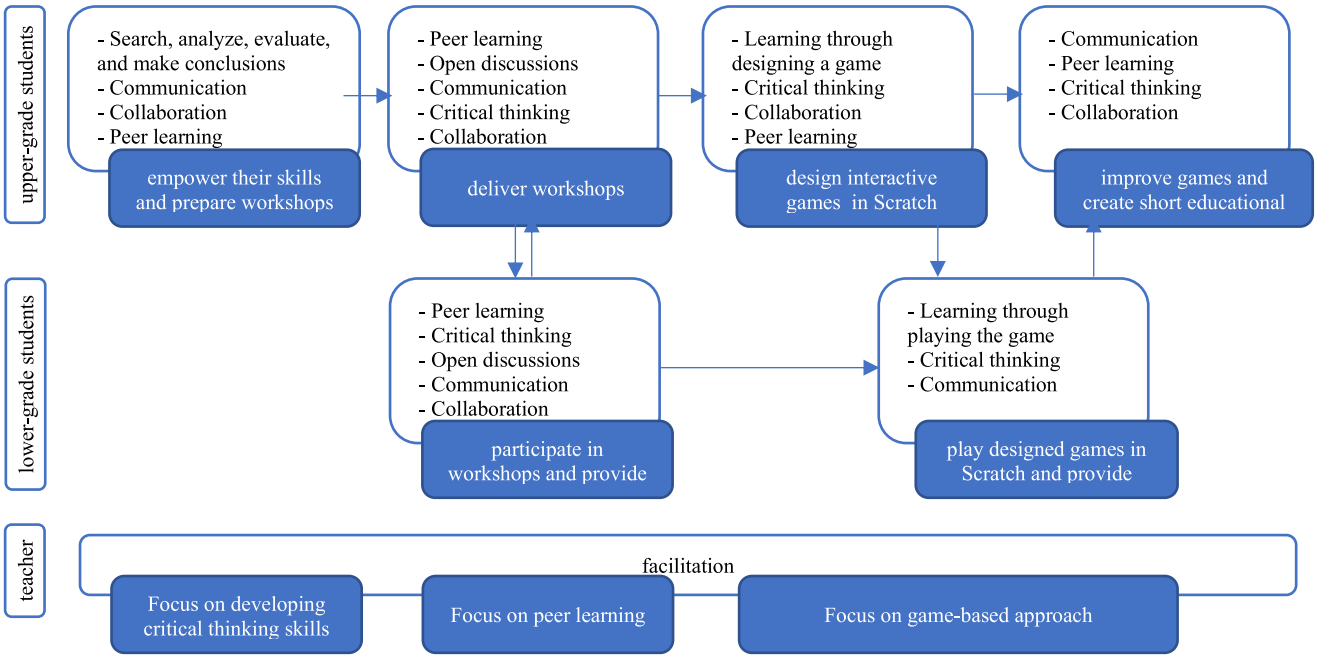

FIGURE 1. Proposed methodological approach for teaching cybersecurity in primary schools.

parties, promoting widespread access to quality cybersecurity education.

To ensure that the correct cybersecurity content is provided with the proposed approach, we involved external evaluators to assess the educational materials that have been developed. These evaluators were independent experts capable of evaluating the implementation progress and providing feedback. In our case, the academic Computer Incident Response Team (CIRT) fulfilled this role. This group of experts responds to computer security incidents and offers support, advice, and assistance to organizations and individuals affected by cyber-attacks or other types of security incidents.

For this study, students' opinions about the development of their critical thinking skills, communication, and collaboration skills as a result of this approach were collected. In addition, their attitudes were also used to determine whether this approach creates an interactive, engaging learning environment. Students' opinions and attitudes were measured using a five-point Likert scale, with answers ranging from "strongly disagree" (1) to "strongly agree" (5). The measured statements concerned the development of critical thinking, communication, and collaboration skills and whether the approach made the learning process more exciting and increased students' engagement. This is a very suitable way to provide a quantitative measurement of students' opinions and attitudes in primary schools because they can easily understand these measured statements and choose level of agreement or disagreement with them.

Furthermore, students' knowledge of given cybersecurity topics was assessed twice, at the beginning and one year after implementing the proposed approach. Finally, a comparison of students' results was used to determine whether implementing peer learning and a game-based approach can lead to the acquisition of long-lasting knowledge and skills. Students' assessment was done in some of the participating schools, in lower grades, on a voluntary basis. The same students were assessed at the beginning and after one year. The results were obtained using multiple-choice tests, focusing on fundamental online safety issues that are part of the curriculum in primary schools. Both tests consisted of three categories of questions: sharing personal information, respecting other people's privacy, and identifying insecure links. We've decided to use multiple-choice questions in the test to obtain quantitative data, which can be easily analyzed, and will ensure standardization and comparability of student responses. Each question was assigned a score of 1 for a correct answer and 0 for an incorrect one, and we have evaluated the mean value of students' answers. The idea was to evaluate the retention time of gathered knowledge and skills, in each category and in general, as a result of this approach.

Additionally, other groups of students from the same schools and academic levels that learn about cybersecurity in a traditional classroom setting were also tested. Those students had no previous experience with peer learning and game-based approach while learning about cybersecurity topics. The idea was to see whether the implemented methodology during cybersecurity education influences long-lasting knowledge acquisition.

All activities involving human participants were in accordance with the ethical standards and laws of the Republic of North Macedonia. Informed consent was obtained from all individual participants included in the study.

TABLE 1. Students' gender distribution, their overall opinions and attitudes and their knowledge of cybersecurity topics.

Aspects of methodological approach	Students' group	Gender		Students' opinions and attitudes towards the approach	Students' knowledge
		Male	Female		
Implementation of peer learning and game-based approach	Upper-grade students	39	37	4.73	0.92
	Lower-grade students	124	139	4.59	0.82
Acquiring long-lasting knowledge	Lower-grade students	53	71	/	0.90
	Lower-grade students after one year	53	71	/	0.95

III. RESULTS

The study of the proposed approach for teaching cybersecurity in primary schools occurred in five North Macedonia schools. Two teachers from each school participated as facilitators, while students from grades 6th to 9th were divided into two groups. The upper-grade students (8th and 9th) enhanced their cybersecurity knowledge and skills, and then created educational materials (lectures and games) to be used to teach lower-grade students (6th and 7th grades). This methodological approach was implemented with 263 students from lower grades (47.15% male and 52.85% female) and 76 students from upper grades (51.32% male and 48.62% female).

Comparation on students' knowledge on cybersecurity topics at the beginning and one year after the implementation of the proposed approach was done with 124 students (42.76% male and 57.26% female). Those students were chosen from three of the participating schools on a voluntary basis from the students that were 6th and 7th grade when the proposed approach was implemented. The overall results, including average values of students' opinions and attitudes about the methodological approach (on a scale from 1 to 5) and the average value of students' knowledge on specific topics (on a scale from 0 to 1), are presented in Table 1.

A. IMPLEMENTATION OF THE APPROACH

Initially, students from upper grades worked in groups and explored, gathered information, discussed it among themselves, analyzed it from different perspectives and made joint conclusions. In this way, students developed their critical thinking, communication, and collaboration skills through peer learning approach. Students empowered their cybersecurity competencies and created different teaching materials (presentations, videos, quizzes, worksheets) and prepared workshops on cybersecurity (Fig. 2).

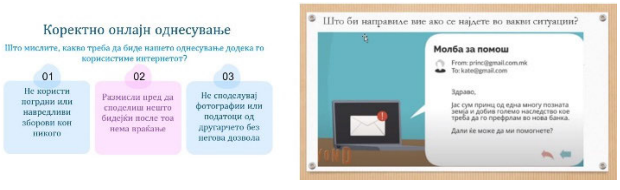

FIGURE 2. Educational materials prepared by upper-grade students.

Lower-grade students learned about cybersecurity topics through lessons delivered by upper-grade students using the already-created educational materials. Through this peer tutoring process, lower-grade students were encouraged to actively participate in the activities, join open discussions and critically think about some challenging situations during their online activities.

According to lower-grade students discussions, upper-grade students managed to identify the most challenging issues on this topic. The teachers were just organizers of the activity and monitored the work, providing feedback and contributing as necessary.

To create an engaging and interactive learning environment where students will learn by playing, upper-grade students created interactive educational games in Scratch concerning cybersecurity (Fig. 3) based on previously identified issues.

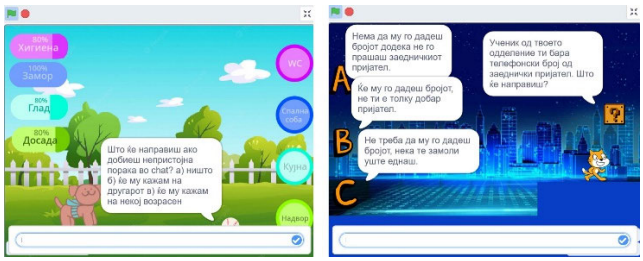

FIGURE 3. Interactive scratch-based educational games created by upper-grade students.

Lower-grade students played those games, and their feedback was used to improve created educational games. Lower-grades students improve their cybersecurity knowledge by playing those games. Educational videos according to the created games were recorded and available to use afterwards. The collection of all the created resources was published online (https://dig-ed.org/open-educational-resources/) and shared with other educators as open educational resources.

B. EVALUATION OF THE METHODOLOGICAL APPROACH

Students' attitudes towards developing their communication, cooperation, and critical thinking skills as the result of the implemented methodological approach were evaluated by questionnaire. In addition, information about establishment of engaging learning environments during peer learning and game-based learning activities was also obtained. Those

results are presented in Table 2, and for each statement, the mean (on a scale from 1 to 5) and standard deviation (SD) are presented, showing the dispersion of students' answers.

TABLE 2. Results of students' attitudes towards implementation of the methodological approach in different age groups.

Statements: This methodological approach has improved my:	Mean (SD)	
	lower-grade students	upper-grade students
critical thinking skills	4.45 (0.77)	4.72 (0.48)
communication skills	4.61 (0.72)	4.67 (0.57)
collaboration skills	4.64 (0.68)	4.72 (0.48)
interest in learning	4.66 (0.70)	4.86 (0.48)
engagement in learning	4.60 (0.71)	4.70 (0.49)

The results show positive attitudes toward implementing peer learning and game-based approaches during cybersecurity education. However, slightly lower values can be noticed in evaluating the approach from lower-grade students compared to their peers from upper grades, especially concerning the development of critical thinking skills.

Furthermore, upper-grade students have more consistent answers, especially concerning developing critical thinking skills, while this dispersion is more significant in lower-grade students. This might result from the different strategies through which students have developed those skills. For example, upper-grade students developed their communication, collaboration and critical thinking skills while creating educational materials (presentations and games), meaning they were all actively involved in the learning process. On the other side, lower-grades students developed their competencies through participation in the activities, which means that their progress is based on their engagement in the activities.

Students' interest and engagement in learning were evaluated very highly by all students, which showed that they liked the process of peer learning and the game-based approach. Hands-on activities during learning make it more motivational and challenging for the students, acquiring their active engagement and persistence during work. This kind of learning is more interesting than other teaching methods, according to most of the students (4.66 – lower-grade students and 4.86 – upper-grade students).

The acquired students' knowledge about cybersecurity was evaluated in three participating schools, in lower grades, on a voluntary basis. Their knowledge concerning sharing personal information, respecting other people's privacy, and identifying insecure links, was assessed twice, at the beginning and one year after the implementation of the proposed approach.

The results about students' knowledge concerning online safety in the three previously mentioned categories (on a scale from 0 to 1) are presented in Table 3. In addition, the standard deviation (SD) of their answers is calculated for each cybersecurity topics, enabling to identify the dispersion of students answers in each of the categories and for each period. The results in Table 3 show that students managed to keep their gathered knowledge after one year. Moreover, acquired knowledge concerning keeping private information safe has increased. Moreover, students have more consistent answers after one year of the implementation of the proposed approach. It leads to the conclusion that the proposed approach can enable acquisition of long-lasting knowledge among students. Additional 87 students (59.77% male and 40.23% female) who learned about cybersecurity in a traditional classroom were also assessed after one year. The idea was to evaluate their knowledge on given topics and conclude whether the implemented methodology influenced acquiring long-lasting knowledge. Table 4 compares the students' knowledge after one year of learning depending on the methodological approach used for teaching cybersecurity topics.

TABLE 3. Students' knowledge of different online safety topics in different time periods.

Questions regarding:	at the beginning	after one year
respecting others online	0.94 (0.23)	0.95 (0.21)
privacy of personal information	0.81 (0.39)	0.97 (0.23)
identifying insecure links	0.94 (0.25)	0.94 (0.16)

TABLE 4. Students' knowledge of different online safety topics after one year of learning according to the used learning approach.

Questions regarding:	The traditional way of teaching	Using peer learning and a game-based approach
respecting others online	0.83 (0.37)	0.95 (0.21)
privacy of personal information	0.87 (0.33)	0.97 (0.23)
identifying insecure links	0.87 (0.33)	0.94 (0.16)

Students that were learning about cybersecurity topics using peer learning and a game-based approach have better knowledge than those learning in a traditional classroom—the most significant difference concern issues related to respecting other people online.

IV. DISCUSSION

Innovative pedagogical approaches should be implemented in education to create engaging learning environments that will increase students' interest and motivation for learning and inspire them to participate actively in classroom activities. Results presented in Table 2 show that peer learning led to the creation of an open, involving, and engaging learning community, where students could talk openly about the topic, communicate, and learn from peers, understand each other, and actively participate in the activity. Game-based learning made learning fun and enjoyable for the students. By utilizing a medium that students use daily, their engagement and motivation for learning were achieved. This

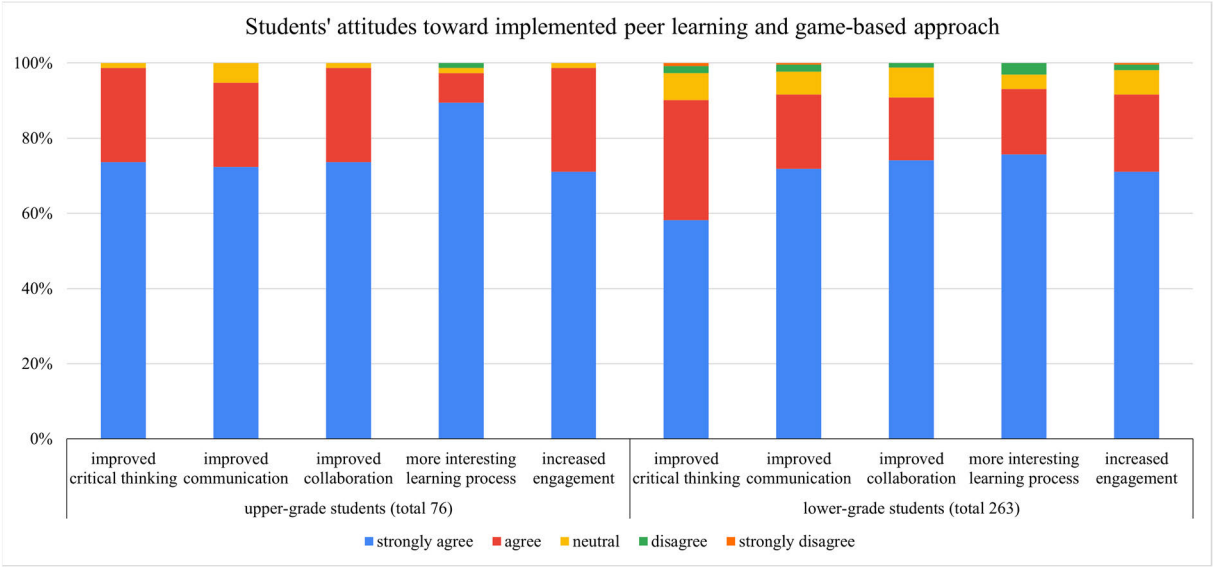

FIGURE 4. Students' opinions and attitudes toward implemented methodological approach.

confirms findings provided by [14], [15], and [16] to be correct in the cybersecurity education as well.

Results clearly show that all students have a positive attitude toward the approach, especially upper-grade students, who actively created educational materials, developing higher-order thinking skills while analyzing information, evaluating and making conclusions within the group (Fig. 4).

Implemented peer learning and a game-based learning approach is very attractive for upper-grade students that were actively involved in the activities during the whole process. It can lead to the conclusion that hands-on activities, where students were involved in creating materials (lectures and games), are most interesting and motivating for students. Those activities develop students critical thinking skills [27], which is the reason why upper-grade students have improved their critical thinking skills more than lower-grade students.

Overall, more than 90% of all students agree with the statements that implementation of the peer learning and game-based approach improves their critical thinking, collaboration and communication skills and that interesting and engaging learning environments can be created in that way (our first research question). This relates to the findings stated in [19], [20], [28], and [29] but confirms them in the cybersecurity education setting as well.

Further analysis of students' attitudes shows that female students have more positive attitudes towards this approach than male students. The analysis of students' attitudes according to gender is presented in Table 5. It can be easily noticed that almost in all statements, female students have assessed this approach slightly better.

Female students (both lower grades and upper grades) have found this approach very interesting and engaging,

TABLE 5. Students' attitudes towards implemented methodological approach based on their gender.

Statements: This methodological approach has improved my:	Lower-grade students		Upper-grade students	
	male	female	male	female
critical thinking skills	4.36	4.53	4.72	4.70
communication skills	4.54	4.67	4.62	4.73
collaboration skills	4.52	4.74	4.62	4.88
interest in learning	4.55	4.76	4.79	4.91
engagement in learning	4.49	4.71	4.54	4.85

which has developed their communication skills. The only statement that male students from upper grades have assessed better (4.72) than female students (4.70) concerns developing critical thinking skills. On the other side, this is a field where all students from lower grades have the slightest improvement due to the approach, especially male students.

Almost all girls from upper grades enjoyed the activities and were actively engaged, developing their collaboration skills. The situation is similar with the answers based on gender in lower-grade students. It is a very interesting result because it proves that using peer learning in combination with a game-based approach can be an excellent way to engage female students in the learning process.

This gives us an insight into our second research question showing that there are gender differences when implementing peer learning and game-based approach and that female students enjoy this approach more and develop their skills at the same time.

A comparison of students' knowledge at the beginning and after one year of implementation of the proposed methodological approach is presented in Fig. 5. It can be concluded that after one year of implementation of the

approach, students' knowledge of cybersecurity is even better than before, and there is smaller dispersion in their answers.

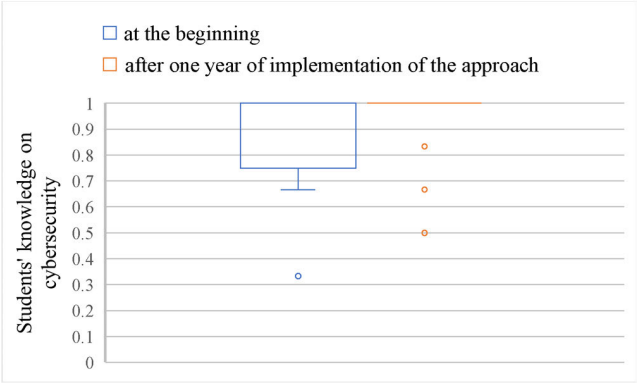

FIGURE 5. Comparison of students' knowledge regarding cybersecurity topics at the beginning and after one year of implementation of peer learning and game-based approach.

On the other hand, a comparison of students' knowledge after one year of learning in the traditional classroom and the implementation of peer learning and a game-based learning approach (Fig. 6) shows that students that have learned in the traditional classroom still have dispersion in their answers. In contrast, the knowledge of students that learn through the proposed methodological approach is increased over time. This confirms findings for increased deeper understanding of the material as stated in [31] and [32] in cybersecurity educational setting.

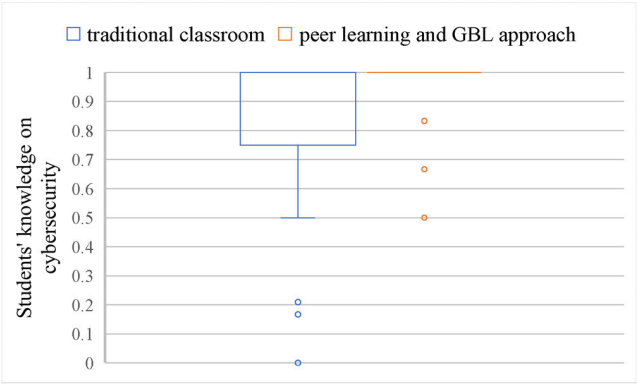

FIGURE 6. Comparison of students' knowledge regarding cybersecurity topics after one year of depending on the implemented approach.

The fact that students manage to keep gathered knowledge and skills after one year (even improved in some segments) leads to a conclusion that a combination of peer learning and game-based learning can be an excellent approach for acquiring long-lasting knowledge and its implementation in real-life situations (third research question).

Further analysis of the student's knowledge of given cybersecurity topics, by gender, at the beginning and after one year showed no significant difference in the retention process depending on the student's gender (Table 6).

TABLE 6. Students' knowledge of given cybersecurity topics at the beginning and after one year of implementation of the proposed approach by gender.

Questions regarding:	at the beginning		after one year	
	male	female	male	female
respecting others online	0.96	0.93	0.96	0.94
privacy of personal information	0.81	0.82	0.96	0.98
identifying insecure links	0.94	0.93	0.92	0.96

All students have improved their knowledge and skills concerning protecting their private information online. Male students have better knowledge about respecting other people's privacy, whereas female students know better how to protect their personal information and behave with suspicious links. However, those are not significant differences.

A comparison of students' results by gender leads to the conclusion that gender has little or no bearing on the used learning approach (Table 7).

TABLE 7. Students' knowledge of given cybersecurity topics after one year of implementation of different learning approaches by gender.

Questions regarding:	The traditional way of teaching		Using peer learning and a game-based approach	
	male	female	male	female
respecting others online	0.81	0.87	0.96	0.94
privacy of personal information	0.88	0.87	0.96	0.98
identifying insecure links	0.90	0.83	0.92	0.96

The overall conclusion would be that there are no gender differences concerning the acquirement of long-lasting knowledge. After one year of learning about cybersecurity, all students (male and female) have similar knowledge on the topics, which improved more in a group of students that practiced peer-learning and game-based learning approach.

The presented methodological approach, utilizing peer learning and game-based instruction, can be easily adapted to various educational contexts and different students' ages. The obtained results give us valuable insight into the benefits of the implementation of the proposed methodology for teaching cybersecurity in primary schools.

The main limitation of the research is that it addresses a small number of participants and provides information about relatively unbalanced data sets (especially concerning the number of students from upper grades compared to lower grades). Implementation of the proposed approach on a larger scale could be useful for validation of the findings. Additionally, students' knowledge and skills were evaluated using multiple-choice tests, which opens the possibility for different kinds of assessment in our future work. The influence of access to technology or students' socio-economic status on the acquisition of long-lasting knowledge of cybersecurity will be an interesting topic to be explored with a larger dataset, too.

V. CONCLUSION

This paper introduces a methodological approach to teaching essential cybersecurity topics in primary education. By implementing a peer learning and game-based approach (first research question), we established an interactive and engaging learning environment to increase students' interest and motivation for the topic and develop their cybersecurity competencies. The peer learning approach involved upper-grade students delivering lectures and creating educational games for their lower-grade peers, fostering learning communities where students openly discussed and shared their knowledge and experiences, learning from one another's diverse perspectives. The game-based approach led to an interactive and engaging learning environment where students developed their critical thinking skills through designing or playing a game and empowered their cybersecurity knowledge.

Students have positive attitudes toward implementing peer learning and a game-based approach during cybersecurity education. They believe this approach has effectively enhanced their communication, collaboration, and critical thinking skills while creating exciting and engaging learning environments. Notably, upper-grade students have slightly more positive attitudes towards the used approach, where they have developed their skills by creating the materials (lectures, workshops, games, videos). This led to the conclusion that hands-on activities, where students are actively involved in the process, are more motivational and challenging, making learning more interesting for them.

Related to the gender differences (second research question), female students have more positive attitudes toward this approach than male students, especially when it comes to developing their communication skills due to active engagement in the learning process. This finding is very intriguing because it proves the efficacy of combining peer learning with the game-based approach in engaging female students in the learning process.

Initial evaluation results after one year of implementing cybersecurity learning indicate that students exposed to peer learning and a game-based approach could retain their knowledge (third research question), with their performance even slightly surpassing their initial levels. Furthermore, their knowledge levels outperformed those of students who received traditional classroom instruction.

The proposed approach has the potential to effectively teach cybersecurity to primary school students, fostering long-lasting knowledge and preparing them for the increasingly digital world.

REFERENCES

[1] C. Balakrishna, "Design considerations for developing a game-based learning resource for cyber security education," in *Proc. Eur. Conf. Games-Based Learn.*, Brighton, U.K., Sep. 2021, pp. 80–89. [Online]. Available: https://oro.open.ac.uk/81179/

[2] S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, and K.-K. Raymond Choo, "The role of national cybersecurity strategies on the improvement of cybersecurity education," *Comput. Secur.*, vol. 119, Aug. 2022, Art. no. 102754, doi: 10.1016/j.cose.2022.102754.

[3] B. J. Blažič, "Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?" *Educ. Inf. Technol.*, vol. 27, no. 3, pp. 3011–3036, 2022, doi: 10.1007/s10639-021-10704-y.

[4] E. Amankwa, "Relevance of cybersecurity education at pedagogy levels in schools," *J. Inf. Secur.*, vol. 12, no. 4, pp. 233–249, 2021, doi: 10.4236/jis.2021.124013.

[5] G. Javidi and E. Sheybani, "K-12 cybersecurity education, research, and outreach," in *Proc. IEEE Frontiers Educ. Conf. (FIE)*, San Jose, CA, USA, Oct. 2018, pp. 1–5, doi: 10.1109/FIE.2018.8659021.

[6] C.-H. Chen, J.-H. Liu, and W.-C. Shou, "How competition in a game-based science learning environment influences students' learning achievement, flow experience, and learning behavioral patterns," *J. Educ. Technol. Soc.*, vol. 21, no. 2, pp. 164–176, 2018. [Online]. Available: https://www.jstor.org/stable/26388392

[7] R. B. Saglam, V. Miller, and V. N. L. Franqueira, "A systematic literature review on cyber security education for children," *IEEE Trans. Educ.*, vol. 66, no. 3, pp. 274–286, 2023, doi: 10.1109/TE.2022.3231019.

[8] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, A. Jøsang, T. Pereira, and E. Stavrou, "Global perspectives on cybersecurity education for 2030: A case for a meta-discipline," in *Proc. Companion 23rd Annu. ACM Conf. Innov. Technol. Comput. Sci. Educ.*, Larnaca, Cyprus, Jul. 2018, pp. 36–54, doi: 10.1145/3293881.3295778.

[9] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues," *Future Internet*, vol. 11, no. 3, p. 73, Mar. 2019, doi: 10.3390/fi11030073.

[10] H.-J. Kam and P. Katerattanakul, "Enhancing student learning in cybersecurity education using an out-of-class learning approach," *J. Inf. Technol. Educ. Innov. Pract.*, vol. 18, pp. 29–47, May 2019, doi: 10.28945/4200.

[11] K. Muir and A. Joinson, "An exploratory study into the negotiation of cyber-security within the family home," *Frontiers Psychol.*, vol. 11, p. 424, Mar. 2020. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fpsyg.2020.00424.c

[12] D. Pencheva, J. Hallett, and A. Rashid, "Bringing cyber to school: Integrating cybersecurity into secondary school education," *IEEE Secur. Privacy*, vol. 18, no. 2, pp. 68–74, Mar. 2020, doi: 10.1109/MSEC.2020.2969409.

[13] N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi, and F. Khalid, "The importance of cybersecurity education in school," *Int. J. Inf. Educ. Technol.*, vol. 10, no. 5, pp. 378–382, 2020, doi: 10.18178/ijiet.2020.10.5.1393.

[14] M. Videnovik, A. Madevska Bogdanova, and V. Trajkovik, "Game-based learning approach in computer science in primary education: A systematic review," *Entertainment Comput.*, vol. 48, Jan. 2024, Art. no. 100616, doi: 10.1016/j.entcom.2023.100616.

[15] D. López-fernández, A. Gordillo, F. Ortega, A. Yagüe, and E. Tovar, "LEGO serious play in software engineering education," *IEEE Access*, vol. 9, pp. 103120–103131, 2021, doi: 10.1109/ACCESS.2021.3095552.

[16] Z. Yu, M. Gao, and L. Wang, "The effect of educational games on learning outcomes, student motivation, engagement and satisfaction," *J. Educ. Comput. Res.*, vol. 59, no. 3, pp. 522–546, Jun. 2021, doi: 10.1177/0735633120969214.

[17] L. V. Mezentseva and E. Al, "Game-driven learning in the digital age: A systematic review and meta-analysis," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 10, Apr. 2021. [Online]. Available: https://turcomat.org/index.php/turkbilmat/article/view/4747

[18] S. George, "Games, simulations, immersive environments, and emerging technologies," in *Encyclopedia of Education and Information Technologies*, A. Tatnall, Ed. Cham, Switzerland: Springer, 2020, pp. 807–816, doi: 10.1007/978-3-030-10576-1_36.

[19] W. Toh and D. Kirschner, "Self-directed learning in video games, affordances and pedagogical implications for teaching and learning," *Comput. Educ.*, vol. 154, Sep. 2020, Art. no. 103912, doi: 10.1016/j.compedu.2020.103912.

[20] D. Zhao, C. H. Muntean, A. E. Chis, and G.-M. Muntean, "Learner attitude, educational background, and gender influence on knowledge gain in a serious games-enhanced programming course," *IEEE Trans. Educ.*, vol. 64, no. 3, pp. 308–316, Aug. 2021, doi: 10.1109/TE.2020.3044174.

[21] M. Rjiba and L. C. Belcadhi, "Self-assessment through serious game," in *Proc. 5th Int. Conf. Inf. Commun. Technol. Accessibility (ICTA)*, Marrakech, Morocco, Dec. 2015, pp. 1–6, doi: 10.1109/ICTA.2015.7426920.
[22] Y. C. Liu, W.-T. Wang, and T.-L. Lee, "An integrated view of information feedback, game quality, and autonomous motivation for evaluating game-based learning effectiveness," *J. Educ. Comput. Res.*, vol. 59, no. 1, pp. 3–40, Mar. 2021, doi: 10.1177/0735633120952044.
[23] M. Videnovik, T. Vold, L. Kiønig, and V. Trajkovik, "Design thinking methodology for increasing quality of experience of augmented reality educational games," in *Proc. 18th Int. Conf. Inf. Technol. Based Higher Educ. Training (ITHET)*, Magdeburg, Germany, Sep. 2019, pp. 1–9, doi: 10.1109/ITHET46829.2019.8937385.
[24] T. H. Laine and R. S. N. Lindberg, "Designing engaging games for education: A systematic literature review on game motivators and design principles," *IEEE Trans. Learn. Technol.*, vol. 13, no. 4, pp. 804–821, Oct. 2020, doi: 10.1109/TLT.2020.3018503.
[25] S. Chandra and S. Palvia, "Online education next wave: Peer to peer learning," *J. Inf. Technol. Case Appl. Res.*, vol. 23, no. 3, pp. 157–172, Jul. 2021, doi: 10.1080/15228053.2021.1980848.
[26] S. Gamlath, "Peer learning and the undergraduate journey: A framework for student success," *Higher Educ. Res. Develop.*, vol. 41, no. 3, pp. 699–713, Apr. 2022, doi: 10.1080/07294360.2021.1877625.
[27] C. Lim, H. A. Jalil, A. Ma'rof, and W. Saad, "Peer learning, self-regulated learning and academic achievement in blended learning courses: A structural equation modeling approach," *Int. J. Emerg. Technol. Learn.*, vol. 15, no. 3, pp. 110–125, Feb. 2020. [Online]. Available: https://www.learntechlib.org/p/217022/
[28] V. D. Tran, "Does cooperative learning increase students' motivation in learning?" *Int. J. Higher Educ.*, vol. 8, no. 5, p. 12, Jul. 2019, doi: 10.5430/ijhe.v8n5p12.
[29] R. C.-Y. Loh and C.-S. Ang, "Unravelling cooperative learning in higher education," *Res. Social Sci. Technol.*, vol. 5, no. 2, pp. 22–39, May 2020, doi: 10.46303/ressat.05.02.2.
[30] M. A. Qureshi, A. Khaskheli, J. A. Qureshi, S. A. Raza, and S. Q. Yousufi, "Factors affecting students' learning performance through collaborative learning and engagement," *Interact. Learn. Environ.*, vol. 31, no. 4, pp. 2371–2391, May 2023, doi: 10.1080/10494820.2021.1884886.
[31] K. Utha and S. Rinzin, "Peer-learning: An alternative teaching pedagogy for highly teacher centered classes," *Int. J. English Literature Social Sci.*, vol. 4, no. 5, pp. 1520–1529, 2019, doi: 10.22161/ijels.45.41.
[32] A. R. Carvalho and C. Santos, "Developing peer mentors' collaborative and metacognitive skills with a technology-enhanced peer learning program," *Comput. Educ. Open*, vol. 3, Dec. 2022, Art. no. 100070, doi: 10.1016/j.caeo.2021.100070.
[33] C. Nerantzi, "The use of peer instruction and flipped learning to support flexible blended learning during and after the COVID-19 pandemic," *Int. J. Manage. Appl. Res.*, vol. 7, no. 2, pp. 184–195, 2020. [Online]. Available: http://ijmar.org/v7n2/20-013.html

MAJA VIDENOVIK received the master's degree concerning educational management on the topic "Managing the ICT Integration in Education," in 2011. She is currently pursuing the Ph.D. degree with the Faculty of Computer Science, Ss. Cyril and Methodius University in Skopje.

She is an Engineer of informatics and a Professor of informatics in primary school in Skopje, Macedonia, dedicated to lifelong learning and has participated in around 100 different kinds of conferences, workshops, seminars, training, courses, and webinars. She is the author of around 20 articles concerning ICT integration in the classroom. She has been a Teacher Trainer on different topics concerning the innovative use of ICT in education, a local expert, and an External Associate of the Bureau for Development of Education. She is a Founder of the NGO "Center for Innovation and Digital Education," she is interested in using ICT for creating interactive learning environments and using educational games in the learning process.

VLADIMIR TRAJKOVIK received the Ph.D. degree from Ss. Cyril and Methodius University in Skopje, in 2003. He is currently a Professor with the Faculty of Computer Science and Engineering. He has published four books as the author or editor, 16 chapters in different books published by international publishers, and more than 60 respectable journals and more than 160 conference papers. He has more than 1100 citations, with an H-index of 18, with research interests mainly focused on two areas: connected health and ICT in education. He has participated in or coordinated more than 60 national and international ICT projects.

TONE VOLD is currently an Assistant Professor who lectures with Inland Norway University of Applied Science, Norway, in courses within knowledge management, organizational learning, informatics, and systems engineering. She is working on her Ph.D. within the area of enterprise development and work life research, doing research on involving students in their own learning process to prepare for work life in organizations.

LINDA VIBEKE KIØNIG is currently an Advisor with Inland Norway University of Applied Sciences, Inland School of Business and Social Sciences. Her main areas are the adaptation of learning arenas to the needs of the work life regarding knowledge and methodology. Her areas of innovation, entrepreneurship and leadership, and the learning processes through project work based on the students' own experiences are in focus. She has a background as the Deputy Major in several Norwegian municipalities. Her research areas also include positive deviance in work on crisis management and preparedness for crisis in the public sector and using games in the real estate education program.

ANA MADEVSKA BOGDANOVA received the Ph.D. degree, in 2003. She is currently a Full Professor with the Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University of Skopje, North Macedonia. Her current research interests include the domain of data science, intelligent systems, connected health, biosensors, and ICT in education.

SONJA FILIPOSKA received the Ph.D. degree from the Faculty of Electrical Engineering and Information Technologies, in 2009. She is currently a Full Professor with the Faculty of Computer Science, Ss. Cyril and Methodius University in Skopje. She has been actively taking part in a number of research projects related to e-infrastructure, networking, and ICT education. During her professional career, she has authored more than 100 research papers published in conference proceedings and journals. Her main research interests include e-services, orchestration of systems, complex networking, and security.