Cyber Kids A Video Game For Rassing Cyber Security Awareness In Children

[1] G.MOUNIKA, [2] A. POOJITHA, [3] K. SREEJA, [4] S. AKHILA,[5] J. SANTHUBAI,[6] G. LAXMI PRASANNA

[1] Assistant Professor, Department of Computer Science and Cyber Security, Princeton Institute of Engineering & Technology for Women, Hyderabad, India

[2,3,4,5,6] B. Tech Students, Department of Computer Science and Cyber Security, Princeton Institute of Engineering & Technology for Women, Hyderabad, India

Abstract:

In most countries, a large percentage of children between the ages of eight and thirteen have access to a mobile device at home, where monitoring and supervision by a trusted adult is not enough, so statistics on children victimized by bullying and damage to the integrity of their personal data have been increasing considerably. In this work, we design and develop a serious game, a playful application that integrates and delivers educational content on cyber security to users aged 8 to 12 years, allowing them to have basic ideas about the responsibilities that the use of current technologies entails. The contents raise awareness about the use of strong passwords and vulnerabilities identification through gamification techniques to ensure both learning and entertainment.

I.INTRODUCTION

In today's increasingly digital world, children are introduced to the internet and digital devices at an early age. From online learning platforms to mobile gaming apps and social networks, children engage with the digital realm daily. However, this exposure comes with cybersecurity threats such as cyberbullying, identity theft, online predators, and exposure to inappropriate content. Unfortunately, children are often unaware of the risks and are ill-equipped to recognize or respond to these threats. Traditional cybersecurity education is often too technical or boring for young learners.

Therefore, it is crucial to find child-friendly, engaging, and interactive methods to instill cybersecurity knowledge. Video games have emerged as one of the most effective tools for education, especially for children. They combine interactivity, visual appeal, and gamified learning, which promotes better retention and active participation. The Cyber Kids game aims to teach children the fundamentals of cybersecurity—such as password safety, stranger danger online, phishing scams, digital footprints, and respectful online behavior—through immersive storytelling and gameplay mechanics tailored to their age group. This research and development effort aligns educational theory with cybersecurity objectives using the power of game-based learning.

II.LITERATURE SURVEY

Several researchers have explored gamification and interactive media as means to teach cybersecurity. Zhong et al. (2018) demonstrated that games significantly improve cybersecurity awareness among students compared to traditional workshops. Garcia & Silva (2020) highlighted the potential of storytelling-based games to reinforce moral and safety values in digital behavior. In their work, “Cybersecurity4Kids,” Lee et al. (2019) showed how children aged 8–12 learned about safe internet habits more effectively through engaging games.

Research also supports the idea that cognitive development stages must be considered while designing educational tools for children. Vygotsky’s theory of the “Zone of Proximal Development” suggests that children learn best when tasks are slightly above their current knowledge level, guided by feedback—something video games naturally provide through levels and challenges. Recent initiatives such as “Interland” by Google and “Cyber Awareness Adventures” by Microsoft use mini-games to teach topics like phishing and password hygiene. However, most existing solutions lack localization, cultural relevance, or coverage of emerging cyber threats. Hence, there is a pressing need for regionally tailored, curriculum-integrated, and accessible games like Cyber Kids to reach young learners globally.

III.EXISTING SYSTEM

Existing systems for cybersecurity education typically include classroom-based training, parental control tools, and instructional videos. Although helpful to an extent, these methods often fail to engage children or present content in a relatable manner. Educational institutions may conduct annual awareness sessions, but retention among children remains low due to lack of interactivity. Applications such as “SafeSurfing” and “Internet Safety for Kids” deliver passive content like text quizzes or videos but do not involve the child actively in decision-making scenarios.

Some schools have integrated simplified coding or internet safety modules, but they are rarely comprehensive and often designed for older students. Moreover, existing games in the cybersecurity domain are often directed at teens or adults, containing complex concepts or dull interfaces that do not appeal to younger minds. The absence of a gamified, age-appropriate, story-driven solution means children lack continuous exposure to cyber safety principles in their formative years, leaving them vulnerable.

IV.PROPOSED SYSTEM

The Cyber Kids video game introduces an interactive learning platform designed specifically for children aged 6–12. The system is built as a 2D or 3D adventure game featuring animated characters, quests, and scenarios that mimic real-life online interactions. Key components of the game include:

1. Character-Based Narratives – Players take on the role of a “Cyber Hero” who explores different virtual environments such as “Social Media Island,” “Password Vault Jungle,” and “Phishing Cave.”
2. Mini-Games and Challenges – Activities include creating strong passwords, identifying fake messages, stopping cyberbullies, and understanding digital footprints.
3. Reward System – Points, badges, and progress levels keep players motivated while reinforcing positive behaviors.
4. Adaptive Difficulty – AI-driven difficulty adjustment ensures that the learning remains challenging yet achievable.
5. Parental Dashboard – Allows parents or teachers to track learning outcomes, time spent, and areas where children need improvement.

The game is developed using game engines like Unity or Godot, integrated with real-world cybersecurity scenarios tailored to child comprehension. Each level unlocks only after learning-based objectives are completed, ensuring both skill development and behavioral reinforcement. Moreover, voice narration, multi-language support, and visual instructions make it accessible to children with varying literacy levels.

V.SYSTEM ARCHITECTURE

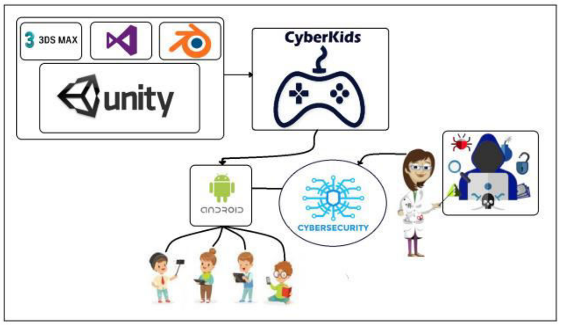


Fig 5.1 System Architecture

The image illustrates the system architecture of the “CyberKids” game, designed to raise cybersecurity awareness among children through an interactive and engaging platform. At the top, the development framework is showcased, highlighting tools such as Unity, 3DS Max, Visual Studio, and Blender—which are widely used for game development, 3D modeling, and scripting. These tools collaboratively contribute to the design and development of the CyberKids video game, indicated at the center with a game controller icon.

The developed game is then linked to an Android platform, showing that the final application is deployed as a mobile app, ensuring accessibility to children using smartphones and tablets. The diagram visually represents children at the bottom left—depicting the primary users of the system, who engage with the CyberKids application on their devices.

In the middle of the architecture is a central cybersecurity hub, which represents the educational content and threat simulations integrated into the game. This includes core topics such as password safety, online etiquette, recognizing phishing attempts, and understanding privacy settings. The cybersecurity module connects both to the game system and the educational agent (a character of a woman/scientist)—symbolizing interactive guidance within the game that helps explain threats and educates users.

Finally, the right side of the image shows a hacker/attacker character, representing potential cybersecurity threats that children face online. This part of the system introduces in-game scenarios where children learn how to identify and mitigate cyber risks in a gamified environment. The entire diagram demonstrates a flow from development tools to game creation, then to deployment, followed by interaction, education, and response to threats, forming a complete loop of learning, simulation, and behavioral reinforcement in the field of cyber security awareness for children.

VI.IMPLEMENTATION

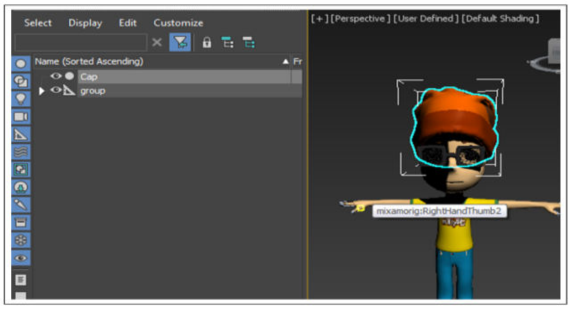

Select
Display
Edit
Customize
Name (Sorted Ascending)
Fr
Cap
group
[+] [Perspective] [User Defined] [Default Shading]
mixamorig:RightHandThumb2

Fig 6.1

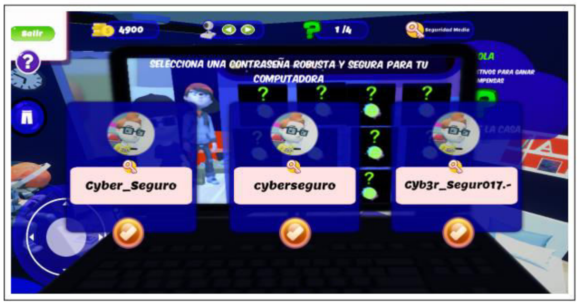

SELECCIONA UNA CONTRASEÑA ROBUSTA Y SEGURA PARA TU COMPUTADORA

Fig 6.2

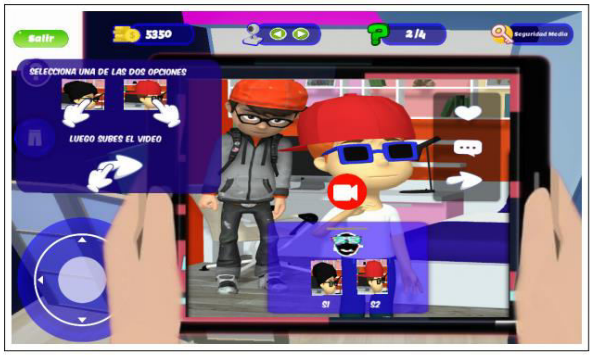


Fig 6.3

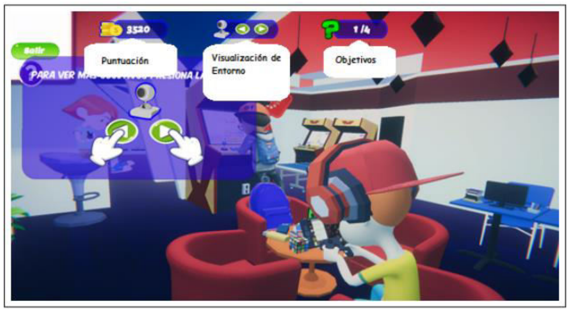
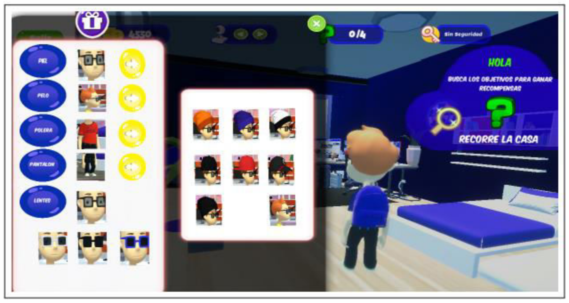
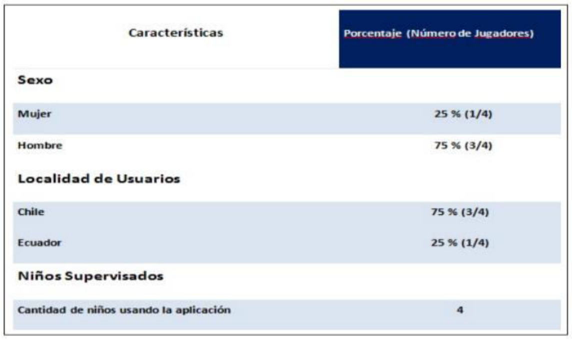


Fig 6.4





Características	Porcentaje (Número de Jugadores)
Sexo	
Mujer	25 % (1/4)
Hombre	75 % (3/4)
Localidad de Usuarios	
Chile	75 % (3/4)
Ecuador	25 % (1/4)
Niños Supervisados	
Cantidad de niños usando la aplicación	4

Fig 6.6

VII.CONCLUSION

The Cyber Kids video game represents a novel and effective approach to instilling cybersecurity awareness among children. Unlike traditional methods, this game promotes active learning through immersive gameplay, reinforcing both knowledge and good digital habits. It bridges the gap between entertainment and education while addressing a critical social issue—the safety of children in the digital world. The proposed system fosters early cybersecurity consciousness, empowering children to make informed and safe choices online. The implementation of this system can significantly reduce the risk of children falling prey to cyber threats and foster a generation that is not just tech-savvy, but also cyber-aware

VIII.FUTURE SCOPE

The potential for Cyber Kids is vast. In future versions, the game can:

- Be integrated into school curriculums as an official digital safety module.
- Offer multi-player functionality to simulate social media environments and peer interactions.
- Include AI-generated new scenarios based on current cyber threat trends.
- Expand to virtual and augmented reality (VR/AR) to enhance immersion and engagement.

- Offer specialized modules for children with learning disabilities to ensure inclusivity.
- Collaborate with law enforcement or cybercrime units to simulate real-world cybercrime prevention techniques.
- Be localized into regional languages and customized for different countries' internet safety challenges.
- Launch a global leaderboard or inter-school competitions to encourage collective learning.
- Collect anonymized gameplay data to conduct research on children’s online behavior understanding.
- Provide certification or e-badges that validate children's knowledge of cybersecurity fundamentals.

IX.REFERENCES

1. Zhong, B., Wang, Q., Chen, J., & Li, Y. (2018). Designing a game for cyber security awareness in primary education. *Educational Technology & Society*, 21(3), 75–88.
2. Lee, J., Kwon, D., & Kim, M. (2019). Cybersecurity4Kids: A game-based learning system for children. *Computers & Education*, 142, 103640.
3. Garcia, D., & Silva, L. (2020). Teaching safe Internet behavior to children through storytelling games. *International Journal of Child-Computer Interaction*, 24, 100224.
4. Google. (2020). Be Internet Awesome: Interland. Retrieved from https://beinternetawesome.withgoogle.com
5. Microsoft. (2021). Cyber Awareness Adventures for Kids. Retrieved from https://www.microsoft.com/security/education
6. Vygotsky, L. (1978). *Mind in Society: The Development of Higher Psychological Processes*. Harvard University Press.
7. Kumar, N., & Banerjee, A. (2021). The Role of Gamification in Cybersecurity Education for School Children. *Journal of Educational Computing Research*, 59(6), 1001–1020.
8. Chou, Y. K. (2015). *Actionable Gamification: Beyond Points, Badges, and Leaderboards*. Octalysis Media.
9. Bada, M., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they

fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

10. Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), 7–29.