

**CEBU INSTITUTE OF TECHNOLOGY
UNIVERSITY**

COLLEGE OF COMPUTER STUDIES

Capstone and Software Engineering Proposal

For

CyberKids

CyberKids

Artezuela, Jhudiell Adrian B.

Baguio, John Kenneth B.

Cultura, Jesson Chyd M.

Dedumo, Emmanuel A.

Vequiso, Ashley Josh V.

Dr. Eugene Busico

Adviser

Consultation Schedule: BUSITUE100200

March 6, 2025

EXECUTIVE SUMMARY

CyberKids is an interactive, gamified cybersecurity education platform designed to equip elementary school students with essential skills for safely navigating the digital world. With children gaining access to the internet at an early age, they are increasingly vulnerable to online threats such as privacy violations, password insecurity, phishing scams, and oversharing personal information. Traditional cybersecurity education in schools is often limited, relying on passive learning methods like lectures and quizzes, which fail to engage young learners effectively.

To address this gap, CyberKids integrates game-based learning mechanics to make cybersecurity education both engaging and practical. Unlike conventional cybersecurity awareness programs, CyberKids immerses students in interactive challenges, role-playing scenarios, and digital escape rooms where they learn to identify risks, build strong passwords, and make informed decisions about online safety. Through real-time feedback, adaptive learning pathways, and engaging storytelling, the system ensures that students not only understand cybersecurity concepts but also develop critical thinking and decision-making skills.

The fundamental objectives of CyberKids include the development of cybersecurity awareness, improvement of students' decision-making in online interactions, reinforcement of password security habits, and enhancement of phishing and scam detection skills. The system outlines all required operations, including input, processing, and output. Input data consists of student interactions, gameplay choices, and performance metrics from various cybersecurity challenges. Processing is managed through adaptive difficulty settings. The output data includes improved cybersecurity knowledge, stronger online safety habits, and teacher insights on students progress.

BACKGROUND AND PROBLEM STATEMENT

Description of the Problem or Gap

According to Farzana Quayyum (CyberFamily: A Collaborative Family Game to Increase Children's Cybersecurity Awareness), elementary school students face growing cybersecurity risks as they gain access to digital devices at a young age. These risks include privacy violations, weak password security, phishing scams, and cyberbullying. However, current educational approaches often fail to provide engaging, age-appropriate methods to teach children essential cybersecurity skills. Research by Churairat O'Brien (Teachers' Perceptions About Use of Digital Games and Online Resources for Cybersecurity Basics Education: A Case Study) highlights the importance of integrating digital game-based learning and online resources to enhance students' understanding of cybersecurity concepts, particularly for Grades 4 to 6. Through technology exposure activities, surveys, and interviews, the study identified a gap in effective cybersecurity education tailored to young learners.

In the Philippines, Maria Lolita Manalo (Cybersecurity Awareness and Educational Outcomes of Grade 4 Learners in Davao, Philippines) found a strong correlation ($r = 0.685$, $p < 0.05$) between cybersecurity awareness and academic performance, reinforcing the need for early intervention in cybersecurity education. However, many existing cybersecurity education tools rely heavily on passive learning methods such as articles and videos, which fail to fully engage young learners or promote long-term knowledge retention. Research from the University of Texas at San Antonio (Play It Safe: An Educational Cyber Safety Game for Children in Elementary School) indicates that game-based learning (GBL) is more effective than traditional text-based approaches in teaching cyber safety concepts to children. Despite this, many existing cybersecurity games, such as Google's Interland and FBI Safe Online Surfing (SOS), are primarily quiz-based, limiting their ability to sustain student engagement and promote critical thinking.

Limitations of Existing Solutions

Existing cybersecurity education solutions have several limitations that make it challenging for elementary school students to develop strong cybersecurity awareness and safe online habits. These shortcomings include reliance on passive learning methods, limited interactivity in gamified approaches, lack of real-time feedback, and the absence of a structured progress-tracking system. While some web-based platforms and educational tools aim to teach cybersecurity, they still have significant drawbacks that hinder their effectiveness.

1. Reliance on Passive Learning Methods

Many existing cybersecurity education platforms rely on passive learning methods such as articles, instructional videos, and static quizzes to teach fundamental concepts. However, this approach has several limitations:

- a) **Limited Engagement** – Without interactive elements, students may struggle to stay engaged with text-based or video-driven content. Younger learners benefit more from hands-on, experiential learning rather than passive consumption of information.
- b) **Lack of Knowledge Retention** – Research suggests that students retain information more effectively when they actively participate in the learning process. Traditional methods, such as reading articles or watching educational videos, often fail to reinforce key cybersecurity concepts over time (University of Texas at San Antonio, 2019).

2. Limited Interactivity in Gamified Cybersecurity Solutions

While existing gamified cybersecurity education platforms incorporate quizzes, point-based rewards, and animated scenarios to make learning more engaging. However, these solutions still have several limitations that reduce their

effectiveness in fostering cybersecurity awareness among younger learners:

- a) Lack of Immersive Gameplay – While some cybersecurity games include interactive elements, many still rely on static multiple-choice quizzes rather than fully immersive, decision-based gameplay.
- b) No Real Consequences for Mistakes – Many educational cybersecurity games allow students to retry questions without any penalty, making it possible to guess answers until they succeed.

3. Lack of a Teacher Dashboard







Existing cybersecurity education solutions primarily focus on independent student learning, often lacking integration for teacher oversight or guidance. Without a dedicated teacher dashboard, educators are unable to track student progress, assess comprehension, or provide targeted support.

4. Lack of Personalized and Adaptive Learning Mechanisms

Cybersecurity education solutions often follow a one-size-fits-all approach, lacking personalized and adaptive learning mechanisms. These systems do not adjust to individual student progress, learning styles, or areas of difficulty, which can result in disengagement or ineffective knowledge retention.

5. Limitations of Similar System and Websites

Several existing platforms provide basic cybersecurity education for children, but they have significant limitations that hinder their effectiveness:

| Platform | Limitations |
|--|---|
|  Google Interland | Primarily focuses on quiz-based challenges and predefined tasks, lacking dynamic problem-solving scenarios. |
|  FBI Safe Online Surfing (SOS) | The platform allows users to repeatedly attempt quizzes without any meaningful consequence or adaptive feedback, which can lead to guesswork. |
|  Education Arcade Cybersecurity Game | Primarily designed for older students, making the content less engaging or accessible for younger children. |
|  Code.org | Primarily focuses on coding concepts rather than in-depth cybersecurity education. |
|  Cybersmart Challenge | The platform still depends on passive learning elements like videos, articles, and static scenarios. |
|  Password Zapper Game for Kids | Limited by narrow focus on password security, which may not provide a comprehensive cybersecurity education. |



Spot the Phish

Limited by narrow focus on phishing, which may not fully prepare children for more complex cybersecurity threats.



Space Shelter Google

Primarily focuses on quiz-based challenges and predefined tasks

Justification for the Proposed Solution

Ensuring that children develop strong cybersecurity awareness from an early age is essential in today's digital world. However, as outlined in the Limitations of Existing Solutions, current cybersecurity education platforms rely on passive learning, lack interactivity, and fail to provide teacher oversight or personalized learning experiences. These limitations hinder students' ability to fully engage with and retain critical cybersecurity knowledge.

Our proposed solution, CyberKids, bridges these gaps by offering an interactive, gamified, and adaptive learning experience tailored specifically for young learners. Unlike existing platforms, CyberKids integrates real-world scenarios, a dynamic feedback system, and teacher support features to enhance student engagement and cybersecurity proficiency.

a) Interactive and Scenario-Based Learning

Many current cybersecurity education platforms rely on quizzes and text-heavy lessons rather than immersive learning experiences. CyberKids addresses this issue by integrating hands-on challenges, real-world cybersecurity scenarios, and problem-solving activities that require students to apply their knowledge in simulated environments. Research suggests that interactive learning improves retention and engagement compared to passive learning methods (Brown et al., 2022).

b) Personalized and Adaptive Learning Pathways

Existing solutions often follow a one-size-fits-all approach, failing to accommodate different learning speeds and skill levels. CyberKids incorporates adaptive learning algorithms that adjust the difficulty of exercises based on student progress. This ensures that learners remain challenged but not overwhelmed, fostering a continuous learning experience tailored to their abilities.

c) Integrated Teacher Dashboard for Monitoring and Guidance

Unlike many gamified cybersecurity platforms, which are designed solely for independent student use, CyberKids provides educators with a dedicated teacher dashboard. This feature enables teachers to track student progress, identify areas where additional guidance is needed, and customize lesson plans accordingly. By involving teachers in the learning process, CyberKids promotes a more structured and effective cybersecurity education approach.

d) Consequence-Driven Gameplay to Reinforce Learning

Many existing cybersecurity education games allow students to repeatedly retry quizzes without meaningful consequences, reducing the impact of incorrect answers. CyberKids addresses this by implementing a structured feedback system, where incorrect responses trigger explanations, corrective learning paths, or in-game consequences. This approach encourages students to think critically and understand the reasoning behind correct cybersecurity practices.

In summary, CyberKids offers a comprehensive and innovative approach to cybersecurity education for young learners. By addressing the shortcomings of existing solutions, it ensures that students receive an engaging, adaptive, and teacher-supported learning experience that prepares them for safe and responsible digital citizenship.

PROJECT OBJECTIVES

This section defines the project's goals in a structured and measurable way. It ensures alignment between the solution and the problem it addresses. The objectives are divided into Main Objectives (SMART Goals) and Specific Objectives (Key Deliverables) to guide the development and implementation of the project effectively.

Main Objectives

The main objectives address the key pain points identified in the Problem Statement section. Each objective is designed following the SMART (Specific, Measurable, Achievable, Relevant, and Time-bound) framework, ensuring clear and trackable progress throughout the project's lifecycle.

1. Gamified Cybersecurity Game Levels

This involves creating and launching three interactive game levels within the Roblox platform, each focusing on a key cybersecurity topic: Online Privacy, Password Security, and Phishing Awareness. Each level will have a timer to add a sense of urgency, a scoring system to reward performance, and polling-based leaderboards to foster friendly competition among students. These elements aim to engage students actively, motivate continuous learning, and reinforce cybersecurity concepts through hands-on experience.

2. Student Real-Name Registration

Students will go through a registration process that requires them to provide their real names, which are then linked to their unique Roblox accounts. This approach helps ensure accurate identification and tracking of student progress.

3. Teacher Web Dashboard

A dedicated web-based dashboard will be developed for teachers, offering comprehensive tools to oversee their students' learning journey. This dashboard will provide real-time access to student progress, performance reports, and detailed analytics. Teachers will be able to generate and export reports, identify areas where students struggle, and tailor their instruction accordingly, ensuring effective classroom management and improved learning outcomes.

4. Notification System

Teachers will have the capability to create, send, and manage real-time notifications regarding important student activities or events. This system will support timely communication such as alerting students about upcoming deadlines, achievements, or required actions. It will also allow teachers to keep students engaged and informed, improving responsiveness and participation in the cybersecurity learning program.

Specific Objectives

This section defines the specific objectives of the system, detailing the key functionalities that must be implemented to meet the project's goals. Each objective represents a core feature that contributes to the system's overall usability, security, and effectiveness.

1. Gamified Cybersecurity Game Levels

Design and deploy three Roblox game levels (Online Privacy, Password Security, Phishing Awareness) with timer, scoring, and polling-based leaderboards.

- **1.1 Information Classification Sorting Challenge** - Students drag and drop digital items into "Safe to Share" or "Not Safe to Share" bins. The system starts a timer on level entry, calculates accuracy and completion time, awards points, and submits the result via a REST call.
- **1.2 Password Security Challenge** - Players collect scattered password fragments from treasure chests, assemble them into a strong password, and submit via an API endpoint. The backend scores strength based on complexity rules and returns points, which update the leaderboard.
- **1.3 Phishing Identification Challenge** - In a virtual escape room, students inspect emails, links, and pages for phishing cues. Each "flag" action triggers a transaction that logs the item ID, correctness, and timestamp; scores are tallied and sent to the leaderboard service.

2. Student Real-Name Registration

Develop a registration flow prompting students to enter their real names linked to Roblox IDs and a read-only profile UI showing unlocked levels and cumulative scores.

- o **2.1 Real-Name Registration Transaction** - Upon first login, the game prompts a RESTful POST with {robloxId, realName}; the backend creates or updates the Student record and returns a confirmation.

3. Teacher Web Dashboard

Provide teachers with tools to monitor, report, and manage student progress.

- o **3.1 Level Control Transaction** - Lock/unlock buttons send PUT requests {studentId, levelId, status} to enable or disable access.
- o **3.2 Student Level Reassignment** - A settings UI sends a PATCH {studentId, newLevelId} to move students between levels.
- o **3.3 Report Generation Transaction** - Teachers click “Export CSV/PDF,” triggering a POST that compiles the selected data into a downloadable file.

4. Notification System

Allow teachers to compose and manage real-time alerts for student events.

- o **4.1 Retrieve Notifications** - Teachers see a list of all notifications—new and old—pulled into their dashboard so they can stay informed about key student events.
- o **4.2 Mark Notification as Read/Unread** - Teachers can indicate which alerts they’ve reviewed by toggling a “read” or “unread” status, helping them track which items still need attention.
- o **4.3 Delete Notification** - Outdated or irrelevant alerts can be removed from the dashboard, keeping the notification list clean and focused on what matters.

Scope and Limitations

CyberKids is designed to align with the Grade 5 and 6 computer curriculum taught by Teacher Rosario, covering essential cybersecurity topics. The system will use Roblox as the game engine to develop the interactive cybersecurity learning modules. A separate web-based Teacher Dashboard will be implemented for tracking student progress and generating reports.

Features and Functionalities

- **Core Features:**

- Interactive and immersive learning modules covering online privacy, password security, and phishing awareness.
- Separate platforms for students (via Roblox) and teachers (via the Teacher Dashboard).
- User registration and role-based access for students and teachers.

- **Gamification Elements:**

- **Challenging Activities:** Each module offers unique challenges tailored to specific cybersecurity topics.
- **Point-Based Scoring System:** Students earn points based on accuracy, speed, and challenge completion.
- **Timer System:** Adds urgency and enhances challenge dynamics.
- **Leaderboards:** Ranks students based on performance, promoting healthy competition.

- **Performance Tracking and Reporting:**

- Real-time progress tracking for students.
- A comprehensive Teacher Dashboard for monitoring individual and class performance.
- Report generation and exporting capabilities for in-depth analysis.

How the System Works

The system consists of two separate platforms:

- Students access the cybersecurity learning game via Roblox, requiring only a Roblox account to participate.
- Teachers access the Teacher Dashboard through a dedicated web interface to monitor and evaluate student performance.

User Registration & Authentication

Students and teachers create accounts according to their roles.

- Students create a Roblox account to access the game.
- Teachers create accounts on the Teacher Dashboard (may also use Microsoft Teams account) for secure access. Once registered, they can log in using their credentials to view and analyze class performance.

Cybersecurity Game Mechanics

Students engage in the game through Roblox, starting at Level 1 and progressing through increasingly challenging levels. Each level covers key cybersecurity concepts, reinforcing classroom lessons.

- The game automatically saves their progress, allowing students to resume from where they left off.
- Scores, completion status, and time spent on each level are recorded and stored.
- The game is designed to be immersive, providing instant feedback and rewards based on performance.

Tracking & Performance Evaluation

Student progress is continuously tracked within the game, and performance data is sent to the Teacher Dashboard for detailed analysis.

- **Leaderboard System:** Ranks students based on points, completion time, and other metrics.
- **Teacher Dashboard:** Provides teachers with an overview of student performance, participation, and level completion rates. Teachers can view detailed reports, including individual scores and class progress.

Constraints and Exclusions

Since *CyberKids* is a capstone project, its development and deployment are constrained by various factors, including budget, timeline, and technical expertise. While the system aims to provide a functional career guidance platform, several limitations must be considered:

- **Budget Constraints** – Limited Hosting and Deployment
 - At this stage, *CyberKids* will be hosted on free-tier cloud services to minimize costs. This may lead to limitations in server performance, storage, and concurrent user capacity.
 - Deployment is not yet a primary requirement, so the platform may remain in a local development environment during testing and refinement.
- **Time Constraints** – Limited Feature Implementation
 - With only two months remaining in the project timeline, not all desired features may be fully implemented.
 - Development will focus on core functionalities, such as gameplay mechanics, student progress tracking, and interactive cybersecurity challenges, while some advanced features (e.g., expanded game levels, multiplayer functionality) may be postponed for future iterations.
- **Technical Learning Curve**
 - The team is still in the process of studying system integration, system administration, and testing methodologies. As a result, certain complex functionalities (e.g., advanced game mechanics, real-time progress tracking) may have limited implementation in the current version.
 - Further improvements will require more research and experimentation beyond the scope of the capstone project.
- **Data and Institutional Coverage Limitations**
 - Initially, the platform will be limited to the elementary department, specifically for Grades 5-6 students at Cebu Institute of Technology University. Expanding its coverage to other grade levels or institutions will depend on future developments and potential collaborations with

educational stakeholders.

- CyberKids is designed based on the cybersecurity topics covered by Teacher Rosario for Grade 5 and 6 students, including online safety, responsible computer use, password security, and cybercrime awareness. As a result, the platform may not cover advanced cybersecurity concepts beyond what is taught in the curriculum.

- **Internet and Accessibility Constraints**

- The platform requires both an internet connection and access to a computer lab for elementary students to use effectively.
- An offline mode for the web platform will be explored and implemented if feasible, allowing students to access certain features without requiring a constant internet connection. The platform does not yet have a dedicated mobile application.

- **Not a Replacement for Traditional Learning Methods**

- The system is not designed to replace traditional static learning methods but to supplement them with interactive cybersecurity challenges. Teachers will continue to play a crucial role in guiding students, while the platform serves as a complementary tool to reinforce lessons through hands-on activities.

- **No Guaranteed Engagement**

- While the system is designed to be interactive and engaging, there is no guarantee that all students will find it fully immersive. As the development team is new to game development, some aspects of gameplay may require further refinement. However, the team is committed to continuously improving the experience by refining game mechanics and incorporating feedback from students and educators.

PROPOSED SOLUTION AND METHODOLOGY

Overview of the Software

CyberKids is an interactive cybersecurity education platform designed to teach elementary students (grades 5-6) about online safety through gamification. The platform leverages Roblox, a popular online gaming environment, to deliver immersive, engaging, and interactive learning experiences. By using Roblox's dynamic game engine, CyberKids offers a familiar and captivating environment for students to explore cybersecurity concepts in a fun and memorable way.

Unlike traditional methods that rely on lectures or static materials, CyberKids transforms digital safety lessons into a series of interactive challenges. Students create their own Roblox accounts to access the cybersecurity games, while teachers use a separate web-based dashboard to monitor student progress, evaluate performance, and generate reports. This separation ensures a seamless, role-specific experience for both students and teachers.

The development team is implementing three primary game modules within Roblox, each designed to focus on essential cybersecurity topics through a mix of puzzle and strategy mechanics:

1. Personal Information Sharing (Online Privacy and Safety Module)

Students analyze chat messages, social media posts, and online forms using a drag-and-drop system within the Roblox environment. They categorize information as safe or unsafe to share, earning points for correct classifications. Timed challenges and instant feedback create a sense of urgency and reinforce learning.

2. Password Fortress (Password Security Module)

Students construct a strong password by selecting uppercase letters, numbers, and symbols from a collection of items. A fortress visual within Roblox represents password strength—weak passwords make it vulnerable to simulated hacker attacks, while strong passwords provide greater protection. This visual approach helps students understand the importance of robust passwords.

3. Cyber Escape Room (Phishing and Scam Awareness Module)

Students navigate a virtual escape room inside Roblox, where they identify phishing emails, fake websites, and scam messages. Using an interactive selection system, students must spot security threats to unlock the exit before time runs out. This high-stakes, scenario-based learning environment promotes critical thinking and problem-solving skills.

Through immersive gameplay and real-world scenarios, CyberKids fosters active learning by encouraging students to apply cybersecurity principles in a hands-on, engaging manner. Instant feedback, point-based scoring, and leaderboards motivate students to excel while reinforcing their understanding of safe online behavior.

The Teacher Dashboard provides teachers with detailed insights into student performance, including progress tracking, challenge completion, and overall learning outcomes. Teachers can use the dashboard to generate performance reports and identify areas where students may need additional support.

Technologies and Platforms

To build CyberKids, we will utilize a combination of modern, scalable, and cost-effective technologies. The selected tools and platforms ensure that the system remains interactive, secure, and optimized for young learners while keeping development and deployment efficient.

Client-Side (Frontend) - React

- React.js (Vite) – For building the user interface efficiently.
- ShadCN UI Component- Provides pre-built, modern UI components for a consistent and responsive design.
- Axios - Manages API requests to send and receive data from the backend.
- Vercel - Hosting the frontend for free, providing fast deployments

Server-Side (Backend) – Spring Boot

- Spring Boot (Java) - Framework used to develop the backend of CyberKids.
- Spring Boot (Java) – Used for building and managing the backend of CyberKids.
- Spring Security & JWT – Ensures authentication and secures API endpoints.
- MySQL – Database management system for storing user data, assessments, and recommendations.
- Render – Free cloud hosting service for deploying the backend and database.

Game Engine

- Roblox - Chosen for its beginner-friendly tools, built-in multiplayer support, and Lua scripting, despite the team being new to game development.

Version Control & Collaboration

- Git & GitHub – For collaborative development and version control.
- ClickUp – For project management and tracking.
- Spear and Queueit - For tracking

By leveraging these technologies, CyberKids ensures scalability, security, and a seamless user experience while keeping development costs low. The combination of React, Spring Boot, and the chosen game engine enables us to deliver an interactive and engaging cybersecurity education platform that enhances learning through gamification.

Development Approach

To ensure a structured yet flexible development process, CyberKids will follow an Agile methodology using Scrum-based sprints while including some Waterfall elements for initial planning.

1. Waterfall for Initial Planning & System Design

The early stages of development require clear documentation and architecture, ensuring a solid foundation before coding begins.

- Requirement Gathering – ClickUp will be used to define project milestones, gather requirements, and assign tasks.
- System Architecture & Design – Database models, API endpoints, and UI/UX wireframes will be planned and finalized before moving into development.

2. Agile for Development & Testing (Sprint-based Approach)

Once the system design is complete, development will follow an iterative, sprint-based approach, allowing for continuous feedback and improvement.

- GitHub for Collaborative Development
 - Branch-based workflow (feature branches, pull requests, and code reviews).
 - CI/CD setup for automated testing and deployment.
- ClickUp for Agile Task Management
 - Sprint cycles (e.g., 2-week iterations for feature development).
 - Task tracking, bug reporting, and backlog management.

3. Continuous Integration & Deployment (CI/CD)

To maintain code quality and stability, CyberKids will integrate CI/CD pipelines for automated testing and deployment.

- Frequent merges and deployments via GitHub Actions or manual reviews.
- Ongoing code reviews and testing before merging to the main branch.

This hybrid approach ensures that CyberKids is built on a solid foundation while remaining adaptable to new insights. By leveraging Waterfall for structured planning and Agile for iterative development, we can optimize efficiency, minimize risks, and deliver a robust, engaging, and effective cybersecurity learning platform for young learners.

TARGET USERS, CUSTOMERS, BENEFICIARIES, AND PARTNERS

Intended users

The central user base of CyberKids consists of elementary school students in grades 5 and 6, who are increasingly exposed to digital devices and online platforms. As digital natives, these students interact with technology daily but often lack foundational knowledge of cybersecurity risks, such as privacy violations, phishing scams, weak password security, and cyberbullying (Quayyum et al., 2025).

Traditional cybersecurity education methods rely on passive learning, which fails to capture students' attention or equip them with practical skills. CyberKids addresses this gap by aligning its interactive, game-based learning approach with the topics taught by Teacher Rosario, ensuring that students reinforce key lessons in online safety, responsible digital behavior, and cybersecurity awareness through engaging activities.

Young learners often struggle to recognize online threats and develop safe digital habits. Their limited experience makes them particularly vulnerable to social engineering tactics, harmful online interactions, and security breaches due to weak password management. CyberKids provides hands-on learning experiences that simulate real-world cybersecurity challenges, allowing students to develop critical thinking and problem-solving skills while reinforcing best practices for online safety.

How the solution benefits them

CyberKids provides a comprehensive set of benefits tailored to the needs of grade 5 and 6 students from Cebu Institute of Technology University (CIT-U), ensuring they gain essential cybersecurity skills through an engaging and interactive learning experience.

- **Increased Awareness and Safer Online Behavior**

Many young students unknowingly engage in risky online activities due to a lack of cybersecurity knowledge. CyberKids helps them recognize online threats, create strong passwords, and avoid phishing scams, fostering safer internet habits that protect their personal information and digital identity.

- **Engaging and Interactive Learning Experience**

Traditional cybersecurity education often relies on text-heavy materials that fail to capture students' attention. CyberKids utilizes game-based learning, hands-on challenges, and interactive simulations to teach cybersecurity in a fun and engaging way. This approach makes complex topics more accessible and ensures that students retain knowledge more effectively.

- **Protection Against Online Threats**

With the rise of social media and online gaming, cyberbullying and online harassment have become common issues for young students. CyberKids equips them with strategies to handle online threats and recognize suspicious online interactions, empowering them to navigate the digital world confidently and responsibly.

- **Aligned with CIT-U's Digital Literacy Efforts**

CyberKids seamlessly integrates with CIT-U's curriculum, complementing existing digital literacy programs by providing an interactive and structured approach to cybersecurity education. The platform is specifically designed to reinforce the topics covered in Teacher Rosario's lessons for Grade 5 and 6 students, ensuring that the content remains relevant to their current studies. The game modules align with her curriculum, covering essential topics such as online safety, responsible computer use, password security, and cybercrime awareness. This ensures that students receive a well-rounded foundation in online safety, reinforcing the school's commitment to responsible digital citizenship.

- **Encourages Independent Learning and Critical Thinking**

CyberKids fosters problem-solving skills by presenting real-world cybersecurity challenges that require students to think critically and apply what they have learned in practical scenarios. This hands-on approach enhances their

decision-making abilities and prepares them to handle future online risks independently.

Potential Partners and Stakeholders involved

- **Elementary Schools and School Districts:**

CyberKids is designed for elementary school students, making schools and districts the primary users and beneficiaries, enhancing their cybersecurity curriculum and improving student safety online.

- **Computer Teachers:**

The project requires a teacher dashboard to track student progress; therefore, teachers are key stakeholders in implementing CyberKids effectively, gaining valuable tools and resources to teach cybersecurity, even without specialized training.

- **Parents and Guardians:**

Parents are concerned about their children's safety online, and CyberKids can provide peace of mind while increasing awareness of online risks within the family.

- **Cybersecurity Companies/Organizations:**

Companies specializing in cybersecurity education could partner with CyberKids to provide content, expertise, or funding, promoting cybersecurity awareness to a younger audience.

- **Educational Technology Companies:**

Companies that develop educational software could integrate CyberKids into their offerings, expanding their product portfolio with a comprehensive cybersecurity education solution.

- **Government Agencies (e.g., Department of Education):**

Government agencies may be interested in supporting CyberKids to promote cybersecurity awareness among students, aligning with national cybersecurity initiatives and improving digital literacy.

- **Non-profit Organizations Focused on Child Safety:**

Organizations dedicated to protecting children online could partner with CyberKids to promote the platform and reach a wider audience, advancing their mission of ensuring children's safety in the digital world.

- **Researchers in Education/Cybersecurity:**

Researchers can evaluate the effectiveness of CyberKids and contribute to evidence-based cybersecurity education practices, advancing the field and gaining insights into effective learning strategies.

TECHNICAL REQUIREMENTS

Hardware Requirements

- **Student Machines:** Desktop or laptop with at least an Intel Core i5 (or equivalent), 8 GB RAM, integrated or discrete GPU supporting DirectX 10+, and 2 GB free disk space.
- **Teacher Machines:** Any modern PC or Mac capable of running a modern browser, with 4 GB RAM and 1 GB free disk space.
- **Server Infrastructure:** Cloud instances (e.g., Azure) with at least 2 vCPUs, 4 GB RAM, and SSD storage.

Software Requirements

- **Operating Systems:** Windows 10 or later, macOS 10.15 “Catalina” or later.
- **Game Engine:** Roblox Studio (latest stable release).
- **Backend:** Java 17+, Spring Boot 3.x.
- **Frontend:** Node.js 18+, React 18.x, Tailwind CSS, Shadcn/ui components.
- **Database:** MySQL 8.0+ (primary) or PostgreSQL 13+ (alternative), hosted on Azure Database for MySQL.
- **Containers & Deployment:** Docker Desktop for local development; Render.com for backend; Vercel for frontend.

Network & Connectivity

- **Internet:** Minimum 5 Mbps download / 2 Mbps upload per user for reliable game and dashboard use.
- **APIs:** HTTPS support (TLS 1.2+), RESTful endpoints for game data and dashboard operations.
- **Real-Time:** WebSocket channel for notifications; HTTP polling (every 5 s) fallback.

Security Requirements

- **Authentication:** JWT-based token authentication for API access; Microsoft Teams SSO for teachers.
- **Encryption:** All data in transit secured with TLS; passwords hashed with bcrypt (or equivalent).
- **Access Control:** Role-based permissions ensuring students only see their own data and teachers only their class.

EVALUATION AND SUCCESS METRICS

| Metric Category | Metric | Target |
|------------------------------|---|-----------------|
| Learning Outcomes | Average accuracy across all game levels | ≥ 80% |
| Engagement Metrics | • Completion rate of all three levels | ≥ 90% |
| | • Average session duration | 15 - 20 minutes |
| Teacher Dashboard Usage | CSV/PDF report exports per session | Steady |
| User Adoption & Satisfaction | Student real-name registration compliance | 100% |
| | Student satisfaction score (1-5 scale) | ≥ 4.0 |
| | Teacher satisfaction score (1–5 scale) | ≥ 4.0 |

CONCLUSION

In today's digital age, young students are increasingly exposed to online risks, yet they often lack the necessary knowledge to protect themselves. Many students engage in unsafe online behaviors due to limited cybersecurity education, making them vulnerable to threats such as cyberbullying, phishing, and identity theft. Without an engaging and structured learning platform, they may struggle to develop the skills needed to navigate the digital world safely.

CyberKids is designed to address these challenges by providing an interactive, engaging, and age-appropriate cybersecurity learning experience for grade 5 and 6 students at Cebu Institute of Technology University. Through game-based lessons, real-world simulations, and hands-on activities, the platform ensures that students develop essential cybersecurity awareness and responsible digital habits. By integrating this program into the school's digital literacy efforts, CyberKids helps bridge the gap in cybersecurity education, empowering students to make informed decisions, recognize online threats, and take proactive steps to protect themselves online.

The approval of this proposal is a critical step in enhancing cybersecurity education for young students. With the increasing risks associated with online interactions, CyberKids provides a scalable and innovative solution that equips students with the necessary skills to navigate the internet safely and responsibly. As a capstone project, CyberKids is currently focused on developing its core features, including interactive lessons, gamified challenges, and real-time cyber threat simulations. With the right support and resources, the program can be further improved to expand its reach, refine its educational content, and integrate more advanced cybersecurity training tailored to students' evolving needs.

By approving this proposal, stakeholders will contribute to a safer and more informed digital future for elementary students. This initiative not only enhances students' online safety but also supports the school's commitment to promoting digital literacy and responsible internet use. The development and implementation of CyberKids will be a

significant step toward ensuring that young students have the knowledge and confidence to protect themselves in an increasingly digital world.