“CYBERARENA: A SIMPLIFIED INTERACTIVE VARIETY OF GAMIFIED HACK AND DEFEND PLATFORM FOR CYBERSECURITY LEARNING”

A Capstone Project Documentation

Presented to

The College of Computer Studies

**QUEZON CITY UNIVERSITY**

In Partial Fulfillment

of the Requirements for the Degree

**BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY**

Barbon, Ronnie A.

Basas, Miles Jerome E.

Daniel, Christian Dave T.

Geraldo, Rona L.

Hilario, Janroe

Lloren, Mark Angelo C.

Mangmang, Jay Prince T.

Oronce, Jeff A.

Ramos, John David DG.

Ronquillo, Mcrey M.

Sosmeña, Emerson R.

Villanueva, John Carlos S.

Month Year

APPROVAL SHEET

In partial fulfillment of the requirements for the degree **BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY,** this Capstone project entitled **“CYBERARENA: A SIMPLIFIED INTERACTIVE VARIETY OF GAMIFIED HACK AND DEFEND PLATFORM FOR CYBERSECURITY LEARNING”** has been prepared and submitted by Barbon, Ronnie A., Basas, Miles Jerome E., Daniel, Christian Dave T., Geraldo, Rona L., Hilario, Janroe, Lloren, Mark Angelo C., Mangmang, Jay Prince T., Oronce, Jeff A., Ramos, John David DG., Ronquillo, Mcrey M., Sosmeña, Emerson R.**,** and Villanueva, John Carlos S. who are hereby recommended for project presentation.

**zzzzzzzzzzzzz**

*Capstone Project Mentor*

Approved by the Committee for Project presentation with a notation of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ on (date of defense).

**XXXXXXXXXXXXXXX,**

*Chairperson, Project Presentation Committee*

**XXXXXXXX YYYYYYY**

*Panel Member Panel Member*

Accepted and approved in partial fulfillment of the requirements for the degree **BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY**.

**ISAGANI M. TANO, PHD-ELM, DIT**

*Dean of College of Computer Studies*

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DEDICATION

*(can be tentative and to be completed in Capstone 2)*

ACKNOWLEDGMENT

EXECUTIVE SUMMARY

Title : **CyberArena: A Simplified Interactive Variety of**

**Gamified Hack and Defend Platform for Cybersecurity**

**Learning**

Proponents : **Barbon, Ronnie A.**

**Basas, Miles Jerome E.**

**Daniel, Christian Dave T.**

**Geraldo, Rona L., Hilario, Janroe**

**Lloren, Mark Angelo C.**

**Mangmang, Jay Prince T.**

**Oronce, Jeff A.**

**Ramos, John David DG.**

**Ronquillo, Mcrey M.**

**Sosmeña, Emerson R.**

**Villanueva, John Carlos S.**

Mentor : **AAAAAAAAAA H. AAAAAA, MSIT**

Degree : **Bachelor of Science in Information Technology**

Date Completed : **(Month, year)**

Keywords **:**

(---------PROJECT BRIEF------------------------------)

SUMMARY OF CHAPTERS 1 TO 5

TABLE OF CONTENTS

Title Page ...…………………………...……………………………………………………… i

Approval Sheet…………………………………………………………………………….… ii

Dedication …………………………………………………………………………………… iii

Acknowledgement …………………………………………………………………………. iv

Executive Summary…………………………………………………………………………. v

Table of Contents……………………………………………………………………………. vii

List of Tables…………………………………………………………………………………. ix

List of Figures…………………………….…........................................................................... x

List of Appendices…………………………………………………………………………… xi

[**CHAPTER I: CAPSTONE PROJECT BACKGROUND 15**](#_heading=h.2zzyruf0gxhc)

[Introduction 15](#_heading=h.ee80atbt7u26)

[Project Context and It’s Background 15](#_heading=h.j7pskkvl1fki)

[Project Purpose and Description 15](#_heading=h.rqpa27ou7f07)

[Objective of the Study 15](#_heading=h.9yw00dber9ek)

[Main Objective 15](#_heading=h.5m26vix2bc1q)

[Specific Objectives 15](#_heading=h.xkamu0dhhxxv)

[Scope and Delimitations of the Project 15](#_heading=h.enr73736cg9h)

[Theoretical Framework and Conceptual Framework of the Study 16](#_heading=h.e14cmc8sxqbh)

[Definition of Terms (define operational terms used in the study) 16](#_heading=h.5it8sv2s3iz)

[**CHAPTER II: REVIEW OF RELATED LITERATURE AND SYSTEMS 17**](#_heading=h.cbmx3xxgee4s)

[Brief Introduction (of the chapter) 17](#_heading=h.75n91ymo4v3)

[Related Literature 17](#_heading=h.m26t578dr0ik)

[Related Studies 17](#_heading=h.84doyfyur45m)

[Technical Background 17](#_heading=h.nq7fgpdhjd1x)

[**CHAPTER III: DESIGN AND METHODOLOGY 18**](#_heading=h.sz8e0i1ahom9)

[Brief Introduction (of the chapter) 18](#_heading=h.t5jlffvyu3q7)

[Methodology 18](#_heading=h.12769vgxd7n8)

[Requirement Analysis 18](#_heading=h.cdg35ud5gdon)

[Requirement Documentation 18](#_heading=h.rafjhm4z4ej3)

[Design of Software, Systems, Product and/or Processes 19](#_heading=h.nu08bn913zk6)

[Development and Testing 19](#_heading=h.6leuw4gx9np9)

[Implementation Plan 19](#_heading=h.ngpk7vmwdgkr)

[**References 21**](#_heading=h.t2my5oc856nt)

[**APPENDICES 23**](#_heading=h.2123z1jc0cj8)

List of Tables

Table No. Table Title Page No.

1.1

List of Figures

Figure No. Figure Title Page No.

1.1 Conceptual Framework 6

List of Appendices

Appendix Appendix Title Page No.

# CHAPTER I CAPSTONE PROJECT BACKGROUND

## Introduction

In this rapidly evolving era, safeguarding data and systems from digital attacks is essential. Attention to network security and IT security culture can help avert cyber threats. Identity and access management, mobile security, and application security are all essential components of a strong security architecture that aims to stop increasingly sophisticated attacks.

Due to the underlying effects of cyberattacks, the need for fundamental knowledge of cybersecurity is undeniable. However, traditional training frequently prioritizes theory over practical experience, leaving students unprepared for obstacles they may face in the real world (Dhungana et al., 2023). This significant disconnect between theory and practice jeopardizes attempts to develop a robust cybersecurity workforce that can protect against changing threats (Petersen et al., 2020).

The problem addressed in this study revolves around the inadequacy of current cybersecurity education methods to fully prepare learners for practical challenges. Identifying this gap, this system is initially formed with the goal of developing a platform that uses gamified, interactive simulations to engage students in real-world, hands-on experiences while also teaching cybersecurity concepts. Educational studies that highlight how game-based learning may improve motivation, engagement, and the acquisition of practical skills are incorporated into the platform's architecture (Mason et al., 2023).

Furthermore, the platform offers a cutting-edge tool to foster critical thinking, problem-solving, and collaborative abilities, which benefits both training organizations and educational institutions. In addition to improving technical skills, this study cultivates a culture of cybersecurity awareness—a crucial defense mechanism in the digitally linked world of today—by immersing students in real-life cyber defense situations.

In summary, by combining gamified, experiential learning with competitive and cooperative components, CyberArena: A Simplified Interactive Variety of Gamified Hack-and-Defend Platform for Cybersecurity Learning transforms cybersecurity education. It gives users the information, abilities, and mentality they need to protect themselves from changing cyber threats with its varied, realistic challenges and encouraging learning setting. The platform's continuous improvement and validation highlight its potential as a trailblazing paradigm for upcoming advances in cybersecurity training that successfully bridge the theory-practice barrier.

## Project Context and Its Background

Cybersecurity has become one of the most pressing concerns in today’s digital world as threats like phishing, malware, ransomware, and data breaches continue to grow in frequency and sophistication. These attacks not only disrupt personal and organizational activities but also threaten national security, making cybersecurity education more critical than ever. While the demand for skilled professionals is rapidly increasing, traditional teaching methods remain mostly theory-driven, often leaving students with limited exposure to practical, real-world applications. This creates a significant skills gap between classroom knowledge and the ability to respond to actual cyber incidents.

Studies have shown that game-based and experiential learning approaches significantly improve knowledge retention, engagement, and problem-solving abilities compared to conventional instruction. Mason et al. (2023) and Thompson et al. (2023) both emphasized that gamification enhances cybersecurity awareness and practical skills, while also sustaining motivation among learners. However, existing platforms still face limitations, such as accessibility challenges, technical issues, and an overemphasis on competition that can reduce collaboration.

In response, CyberArena: A Simplified Interactive Variety of Gamified Hack-and-Defend Platform for Cybersecurity Learning was conceptualized to provide an innovative solution. The platform integrates realistic simulations of cyberattacks and defense strategies with gamified elements like leaderboards, point systems, achievements, and progression tracking. By combining theoretical foundations with hands-on exercises, it offers learners an engaging and practical environment to apply their skills.

The system directly benefits students, educators, and aspiring cybersecurity professionals by providing opportunities to strengthen their technical competencies, teamwork, and critical thinking. It also supports organizations seeking to enhance cybersecurity awareness among employees. Ultimately, CyberArena addresses the gap in traditional education by offering a more interactive and practical approach, contributing to the development of a cyber-aware and resilient workforce prepared to face today’s evolving digital threats.

## Project Purpose and Description

Nowadays, almost everyone uses things connected to the internet, such as for communication and sharing personal information. Along with this, threats to information security and computer systems are also increasing. Many people, especially beginners in the field of internet safety or cybersecurity, find it difficult to learn important concepts and skills because traditional learning methods are often complicated.

The proponents created this platform called CyberArena simply for this reason. CyberArena is an interactive and simplified platform aimed at making cybersecurity more fun and easier to learn by using game-based elements. In this study, Cyberarena users will learn valuable knowledge about cybersecurity and how to protect themselves from Cyber attacks. They will also understand how attackers think and operate within a system. Using the "hack and defend" concept, this study combines learning and enjoyment to help students and individuals with little knowledge expand their understanding of cybersecurity in a safe and modern way.

The goal of this study is to provide a user-friendly and engaging learning experience that can help prepare young people and beginners in the world of cybersecurity. Through CyberArena, the proponents encourage more individuals to explore and enhance their knowledge in this increasingly important field in today’s digital world.

## Objective of the Study

### Main Objective

To design and develop *CyberArena*, a gamified hack-and-defend platform that enhances cybersecurity education by providing interactive, competitive, and practical learning experiences, bridging the gap between theoretical knowledge and real-world application.

### Specific Objectives

1. **Develop Realistic Cybersecurity Scenarios**

* Design interactive simulations involving malware detection, phishing, ransomware response, penetration testing, and defense strategies.
* Create progressive levels of difficulty suitable for both beginners and advanced learners.

1. **Integrate Gamification Features**

* Implement scoring systems, leaderboards, and achievement badges to boost learner engagement.
* Provide both individual and team-based competition modes to encourage collaboration and healthy competition.
* Enable skill progression tracking and feedback mechanisms for continuous improvement.

1. **Evaluate Platform Effectiveness**

* Conduct usability testing with students, educators, and selected cybersecurity professionals.
* Assess knowledge retention and practical skill enhancement through pre- and post-assessments.
* Gather user feedback to measure engagement, satisfaction, and overall learning experience.

1. **Promote Cybersecurity Awareness and Skill Development**

* Equip learners with practical knowledge to respond effectively to common cyber threats.
* Foster critical thinking, problem-solving, and teamwork through interactive cyber defense exercises.
* Contribute to building a cyber-aware community capable of addressing modern digital challenges.

## Scope and Delimitations of the Project - *(define extent of project and exclusions)*

***Scope***

1. This study covers the development of a gamified platform for learning basic concepts in cybersecurity.
2. The system focuses on a "Hack and defend" approach, where users learn by simulating both attacker and defender roles.
3. The platform includes interactive challenges and learning modules based on real-life cyber scenarios.
4. Cyberarena is designed to have a user-friendly interface suitable for beginners.
5. The system includes a leaderboard and scoring feature to help motivate users while learning.
6. The platform supports self-paced learning, allowing users to learn at their own speed and schedule.
7. The platform only covers basic cybersecurity topics, such as password security, phishing awareness, and basic network safety.
8. The primary target users of the system are students and beginners interested in cybersecurity, not advanced users or professionals.

***Limitation/Delimitation***

1. This study is limited to the development and testing of a prototype platform and does not include full-scale commercial deployment.
2. The evaluation will be conducted on a small group of participants, mainly composed of students and selected individuals from educational institutions, and therefore, the results may not fully generalize to the wider population of cybersecurity practitioners.
3. The simulated challenges in the platform are simplified to align with the beginner to intermediate level of training and are not designed to cover advanced or enterprise-level cyber threats.
4. The platform does not aim to replace professional certifications or formal cybersecurity training programs but rather to serve as a supplementary and innovative tool for learning.

## Theoretical Framework and Conceptual Framework of the Study

This study is anchored on three primary theories:

1. **Constructivist Learning Theory (Piaget, 1972)** – This theory emphasizes that learners build knowledge through experience and active engagement. The proposed gamified “Hack and Defend” platform provides learners with simulated cybersecurity scenarios where they can practice and apply defense strategies, thereby constructing their own knowledge through hands-on experience.
2. **Game-Based Learning Theory (Gee, 2003)** – This theory explains how games can be effective learning tools by increasing motivation, engagement, and retention. The proposed system integrates gaming elements such as challenges, rewards, and interactive scenarios to foster deeper learning in cybersecurity.
3. **Experiential Learning Theory (Kolb, 1984)** – This theory highlights the importance of learning by doing. In the proposed project, learners are not passive recipients of information but active participants in simulated cyber-attack and defense situations, which enhances their skills and understanding of cybersecurity practices.

This study follows the **Input–Process–Output (IPO) Model** to illustrate how the proposed platform functions:

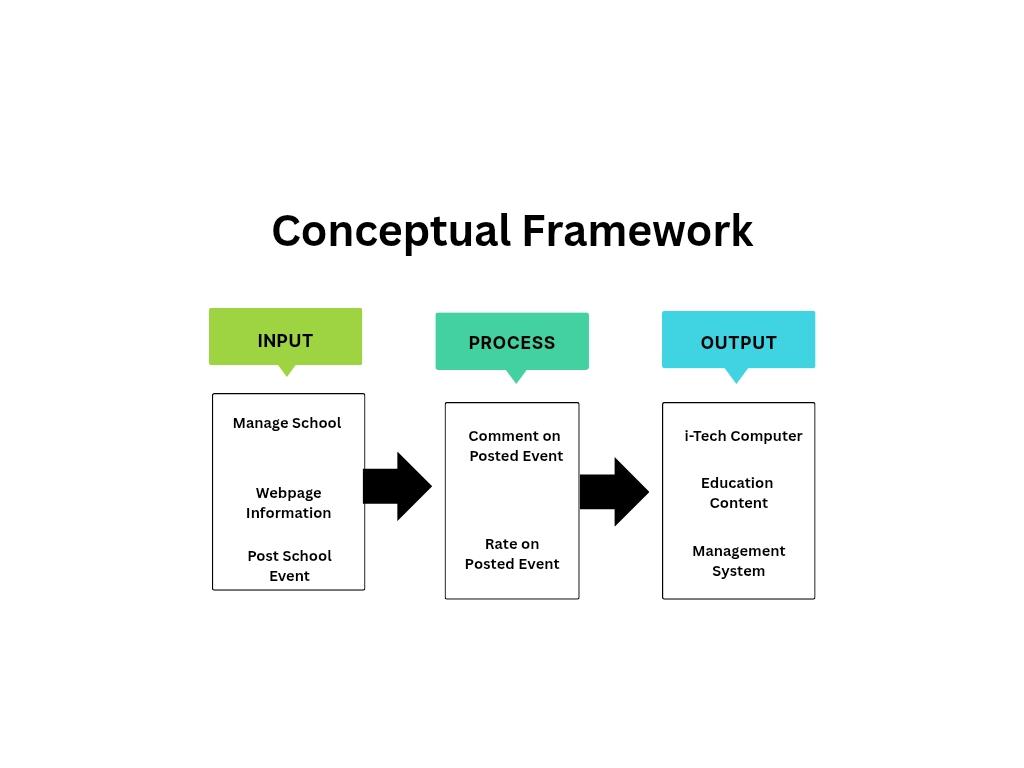


Figure 1.1 CyberArena Conceptual Framework

## 

## 

## Definition of Terms

This section defines the key terms used in the study. The definitions are presented in operational terms to clarify their specific meaning within the context of the CyberArena project.

**Achievement Badges** – Digital rewards granted in CyberArena when users accomplish specific cybersecurity tasks or milestones, promoting engagement and recognition of progress.

**Application Security** – The practice of safeguarding applications from cyberattacks. In CyberArena, users engage in exercises that expose vulnerabilities and apply protective measures.

**Authentication** – The process of verifying a user’s identity before granting access to a system or platform. CyberArena integrates authentication mechanisms to simulate real-world login security.

**Authorization** – The process of granting permissions to authenticated users. Within CyberArena, this ensures that learners can only access the appropriate modules and features.

**CyberArena** – The gamified hack-and-defend platform developed in this study is designed to provide interactive simulations of cyberattacks and defenses to enhance learning in cybersecurity.

**Cyberattack** – Any malicious attempt to compromise computer systems, networks, or data. In CyberArena, learners are exposed to simulated cyberattacks such as phishing, malware, and ransomware.

**Cybersecurity Awareness** – The knowledge and preparedness of users regarding online safety, cyber risks, and protective measures, cultivated through CyberArena’s training modules.

**Cybersecurity Workforce** – Refers to students, educators, and aspiring professionals who are the target beneficiaries of CyberArena, gaining skills and awareness to counter modern cyber threats.

**Data Breach** – The unauthorized access, disclosure, or theft of sensitive information. CyberArena incorporates simulations of breaches to train learners in prevention and response.

**Encryption** – A process of encoding data to prevent unauthorized access. CyberArena uses this concept in exercises to demonstrate how information security is strengthened.

**Firewall** – A network security tool that monitors and filters incoming and outgoing traffic. Within CyberArena, firewalls are discussed in simulations of defense mechanisms.

**Gamification** – The integration of game-based elements such as scoring systems, leaderboards, badges, and progression levels in CyberArena to increase learner engagement and motivation.

**Hack-and-Defend** – A learning approach applied in CyberArena where users take roles both as attackers and defenders in simulated scenarios, promoting a deeper understanding of how cyber threats operate and how they can be countered.

**Interactive Simulation** – Computer-based scenarios in CyberArena that mimic real-world cyber threats such as phishing, malware, or ransomware, enabling learners to apply defense strategies in a safe environment.

**Leaderboard** – A gamification component of CyberArena that ranks users according to their accumulated scores, fostering motivation through competition.

**Malware** – Short for malicious software, it refers to programs designed to disrupt, damage, or gain unauthorized access to systems. CyberArena provides exercises where learners detect and mitigate malware attacks.

**Mobile Security** – Refers to the protection of smartphones and tablets against cyber threats. Within CyberArena, it is addressed through training modules and scenarios that demonstrate secure mobile practices.

**Network Security** – Measures taken to protect a computer network from unauthorized access, misuse, or cyberattacks. In CyberArena, learners apply basic network defense techniques in hands-on activities.

**Phishing** – A cyberattack that uses deceptive messages, often emails, to trick users into revealing sensitive information. CyberArena includes phishing simulations to enhance user awareness.

**Ransomware** – A type of malware that locks or encrypts a victim’s files until a ransom is paid. CyberArena integrates ransomware scenarios to train learners in proper response strategies.

**Scoring System** – A gamified feature in CyberArena that awards points based on the learner’s performance in cybersecurity exercises, encouraging continuous improvement.

**Two-Factor Authentication (2FA)** – An additional security measure that requires two forms of verification for login. CyberArena demonstrates 2FA to emphasize stronger authentication practices.

# CHAPTER II REVIEW OF RELATED LITERATURE AND SYSTEMS

This chapter presents a comprehensive review of literature, studies, and technical background to establish the theoretical and practical foundation of the research and the platform. These sources provide theoretical, empirical, and technical support for the study.

## Related Literature

The rise in the complexity and pervasiveness of cyber threats has greatly contributed to pushing demands for good-quality cybersecurity education. Consequently, methods that offer meaningful engagement through experiential learning, especially "learning by doing," are preferred. Therefore, game-based learning as a learning approach has surged, leading to several studies on exploring its multidimensional influence on cybersecurity education.

Experiential learning is generally labeled as "learning by doing" and is known to be a very successful method for closing the theory-practice gap. According to Kolb's (1984) Experiential Learning Theory, the development of the knowledge and the skills of the learners is at its highest when they are actively involved in the process of learning. In the realm of cybersecurity, experience-based activities like simulations, competitions, and hands-on practice have been very effective in improving not only the technical skills but also the critical thinking and decision-making skills of individuals (Papamartzivanos et al., 2019).

A recent study by Thompson et al. (2023) emphasizes that a student's performance must be monitored over extended periods in game-based training, because a prolonged focus enhances insight into the consistency of learning achievement as well as the effect of regular training on memory retention. Empirical research also proves the efficacy of gamified learning in both higher education and work-related training settings. As an example, Mason et al. (2023) used the Gamified Intelligent Cyber Aptitude and Skills Training (GICAST) program with undergraduate students and recorded valuable improvements in cybersecurity awareness, attitudes, and behaviors. Such outcomes show the significance of gamification in promoting beneficial skills and behavioral change.

Similarly, Johnson and Willey (2022), through their research, highlighted that gamification, when combined with cybersecurity education, greatly enhances problem-solving and critical thinking skills among the learners. Their findings indicated that the competitive and collaborative features, for example, leaderboards and team-based challenges, not only attracted but also engaged the users for a longer duration. Along with this, Park and Lee (2021) revealed that the learning through cybersecurity simulation indicated a more profound understanding as the learners were given the opportunity to take the roles of both the attacker and the defender, which practically confirmed the theory taught.

Moreover, some other researchers focus more on the long-term advantages of the gamified and experiential methodologies. For example, Alshammari et al. (2020) observed that students using hands-on simulation platforms were able to retain the information taught for a longer time compared to those who only followed the lecture-based method. Similarly, Mitropoulos and Karanikas (2021) found that the incorporation of authentic cyberattack scenarios into the training environments significantly elevates the learners’ familiarity with the situation, thus closing the gap between academic preparation and real-world application.

However, challenges still persist in the implementation of a gamified hackathon. Some participants tend to complain about technical problems and the relevance of the content. Furthermore, compulsory training sessions are often marred by experiences of redundancy and loss of interest, which inhibit efficient learning and sabotage a constructive learning culture (Sloman & Borattino, 2007). Thus, CyberArena seeks to balance competitive aspects with cooperation to foster sustained motivation and behavioral transformation rather than forced compliance alone.

The simulation-based environment is another major feature of successful cybersecurity communication. Papamartzivanos et al. ( 2019) showed that students get better knowledge transfer when they are exposed to the practice of the real-world cyber-attack scenario in some virtual laboratories. Such environments enable the learners to apply the techniques of prevention, detection, and mitigation in the same way as in real cyberattacks. The controlled space in these labs ensures that mistakes become learning opportunities, not critical failures.

There is also a growing recognition of the importance of platforms that offer scalable collaborative learning. Vykopal et al. (2021) argued that scalable cloud-based training environments not only make it possible to accommodate a large number of learners but also contribute to making cybersecurity education more accessible. Upset Kindred offers a variety of difficulty levels, allowing both novice and expert users to find appropriate challenges. This is a very important factor in dealing with the worldwide shortage of cybersecurity professionals.

Cybersecurity education should cover the behavioral and cultural aspects, besides the technical part. Alotaibi et al. (2016) are of the opinion that training focused on security culture and awareness is the most important, as even the strongest technical firewalls can be breached if the users are careless. In such games, users are given behavioral lessons in the form of interactive challenges; thus, awareness training can be more engaging and less tiresome than traditional lectures.

CyberArena aims to be part of the emerging gamified cybersecurity training platforms that include interactive learning hackathons, real-world simulations, and gamification components to both motivate users and develop cybersecurity competencies practically and behaviorally. This project will further enhance the gamified hackathon intervention in terms of balancing the amount of cyber theory presented and its applicability to practical hackathons, more importantly, to real-life cases of cyber attacks.

## Related Studies

According to Paculanan et al. (2024), Cyberverse: A Game-Based Learning Application for Cyber Security was developed in response to the growing need for effective cybersecurity education brought about by increasing cyber threats and the lack of engaging tools that integrate theory with practice. The study sought to address the problem of limited awareness and low student engagement in key cybersecurity areas such as password security, phishing, identity theft, encryption, and network protection. Its objectives were to raise awareness of the importance of cybersecurity, help learners distinguish between various cybersecurity topics while playing the application, and identify appropriate tools for assessing the cognitive abilities of gamers. To accomplish this, the researchers employed a quantitative research design and utilized the Agile model for game development, with evaluations conducted using ISO 25010 for technical aspects and the PASS Theory of Intelligence for cognitive assessment involving 60 respondents.

The findings revealed that both gamer and technical respondents strongly agreed that the Cyberverse application enhanced cybersecurity knowledge and effectively engaged cognitive skills. Results confirmed that the game was functional, reliable, and effective in promoting learning. This study is relevant to CYBERARENA: A Simplified Interactive Variety of Gamified Hack and Defend Platform for Cybersecurity Learning as it highlights the effectiveness of gamified approaches in increasing awareness and comprehension of cybersecurity concepts. While Cyberverse emphasized foundational knowledge and awareness, CYBERARENA aims to extend this by providing a simplified yet competitive hack-and-defend environment that allows learners to practice both attack and defense strategies in an interactive and engaging way.

Similarly, Shiaeles et al. (2019) introduced PenQuest: A Gamified Attacker/Defender Meta Model for Cyber Security Assessment and Education to address the limitations of conventional training methods, which often focus heavily on theory and fail to provide students with engaging, hands-on experiences. The study tackled the problem of insufficient exposure to realistic attack-and-defense scenarios, which hindered students’ ability to apply knowledge in practice. Its main objective was to design a gamified meta model where learners could assume the roles of both attackers and defenders, enabling them to experience real-world cyber incidents in a controlled environment. To do so, the researchers developed a role-based simulation that integrated attacker-defender dynamics within a game-based learning framework to assess technical skills and decision-making capabilities.

The findings showed that PenQuest effectively improved participants’ critical thinking, engagement, and practical skills in handling cyberattacks and defenses. In addition, students reported higher motivation and deeper understanding of cybersecurity concepts compared to traditional instruction. This study connects to CYBERARENA as it demonstrates the value of incorporating attacker-defender simulations into cybersecurity education. Whereas PenQuest provided a meta model for gamified assessment and learning, CYBERARENA builds on this approach by offering a simplified, interactive hack-and-defend platform tailored to enhance accessibility and provide Filipino learners with an engaging environment to practice both offensive and defensive cybersecurity strategies.

In line with these gamified efforts, Legg et al. (2023) emphasized that the growing inclusion of computer science in school curricula has increased the demand for practical cybersecurity education. However, teachers face challenges such as limited time, restricted IT resources, and a lack of confidence in delivering practice-based materials. To address these concerns, the researchers conducted workshops with teachers to identify barriers and co-create resources. From this process, they developed a Raspberry Pi–based cyber range, known as the Pi Lab, designed as an isolated and portable infrastructure for teaching offensive and defensive cybersecurity. Using Raspberry Pi devices preconfigured with Kali Linux, Dockerized applications (e.g., OWASP Juice Shop, DVWA, CTFd), and customizable activities, the platform enabled teachers to facilitate red and blue team exercises in a safe, offline environment.

Consequently, the findings indicated that the Pi Lab offered a practical, engaging, and adaptable solution that enhanced teachers’ confidence and students’ understanding of cybersecurity concepts. Activities such as capture-the-flag challenges and red/blue team exercises exposed learners to network scanning, brute force attacks, password security, firewalls, and defense strategies while encouraging active engagement. This work relates to CYBERARENA as both emphasize practice-based, gamified approaches to cybersecurity instruction. While the Raspberry Pi Lab focused on accessible, low-cost classroom integration, CYBERARENA adapts this idea into a gamified hack-and-defend platform that simplifies attack-defense scenarios, aiming to further immerse students in real-world cybersecurity practice.

Moreover, Williams et al. (2024) developed Leveraging Gamification and Game-based Learning in Cybersecurity Education: Engaging and Inspiring Non-Cyber Students to address the shortcomings of lecture-based teaching, which often fails to engage learners—particularly those from non-technical backgrounds. The study identified gaps in existing gamified platforms, such as challenges being overly technical, isolated, and lacking narrative coherence. To overcome these issues, the researchers designed two Capture-the-Flag (CTF) frameworks: an open-ended CTF and a story-based CTF. These were intentionally structured to be inclusive for a diverse student population, ranging from undergraduates to postgraduates, and even those outside of computer science. The methodology involved designing challenges of varying difficulty levels, integrating narrative elements, and facilitating collaborative, team-based problem-solving.

The results revealed that both formats significantly enhanced engagement, critical thinking, and motivation among participants, while also increasing interest in pursuing cybersecurity studies among non-cybersecurity students. Likewise, feedback highlighted the educational value of narrative-driven challenges and the effectiveness of connected tasks in fostering deeper understanding. This study contributes to CYBERARENA by reinforcing the effectiveness of gamification in teaching cybersecurity, particularly through structured CTF activities. While Williams et al. emphasized inclusivity and narrative-driven design, CYBERARENA incorporates this approach into a simplified hack-and-defend platform, aiming to provide Filipino learners with practical yet engaging exposure to both offensive and defensive cybersecurity strategies.

On the other hand, Thombre and Velankar (2022) explored Gamification by Students: An Effective Approach to Cyber Security Concept Learning as a way to engage millennial learners who are less motivated by traditional lecture-based approaches. The study focused on final-year undergraduate students in an Information and Cyber Security course, where low student engagement and limited development of critical thinking skills posed significant challenges. Its objective was to enhance learning by having students design and implement their own cybersecurity games based on concepts such as the CIA triad, network security, and protocols. The methodology required students, in pairs, to brainstorm, prototype, and refine games with feedback from peers and faculty, assessed through the Octalysis gamification framework and evaluated using rubrics focused on creativity, content, rules, and collaboration.

As a result, findings indicated that students were highly motivated by the game design activity, with 68% rating it as excellent. Results also showed improved understanding of cybersecurity concepts, stronger problem-solving skills, and enhanced collaboration. Importantly, the study emphasized that the most valuable learning occurred during the design process, as students applied cybersecurity knowledge to create functional and engaging games. This connects to CYBERARENA as it illustrates how active, gamified learning can significantly improve motivation and knowledge retention. While the focus was on student-created games for peers, CYBERARENA advances this idea by providing a ready-made, simplified hack-and-defend platform that promotes practical learning through attacker-defender simulations.

## Technical Background

| **Software** | **Specification** | **Descriptions** |
| --- | --- | --- |
| Operating System | Windows 10 | A widely used operating system that is compatible with most programs and applications. |

| **Hardware** | **Specification** | **Descriptions** |
| --- | --- | --- |
| Processor | AMD Ryzen 5 3400g | A powerful quad-core processor designed for multitasking and smooth performance. |

| **Other Technology Used** | **Specification** | **Descriptions** |
| --- | --- | --- |
| Processor | Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz (x64) | A quad-core high-performance processor built for multitasking and optimized system speed. |

# 

# 

# 

# 

# 

# 

# 

# 

# 

# CHAPTER III DESIGN AND METHODOLOGY

In this chapter, the proponents outline the methodological approach that will be used to develop this project. It includes requirement analysis with sample techniques and current technical situations, as well as requirement documentation that specifies the project's scope. The chapter also discusses the system design, development, and testing procedures, as well as the data analysis plan, before concluding with the implementation plan to ensure effective deployment of the platform.

## Methodology

This chapter establishes the methodology used for the design and development of the CyberArena platform. In this study, a linear and systematic Waterfall Model of the Software Development Life Cycle (SDLC) will be utilized. The Waterfall Model comprises six phases: planning, analysis, design, coding, testing, and deployment. This was the most ideal and effective model, as it provides a definite framework for the systematic development of a platform, ensuring that each phase is taken into consideration during its implementation before proceeding to the next phase.

This platform will be developed through its different stages, which starts with planning. This includes setting objectives, defining the scope, and reviewing related literature to validate the platform's relevance. With the technical examination of the present situation, identification of user needs, and development of requirements, both functional and non-functional, to cover practical gaps in cybersecurity education. The stage progress was measured by the extent and the clarity of the requirements documented.

After the requirements were defined, the design phase worked on the system architecture, user interface, and gamification ideas. Hence, a simple depiction of how the program would operate ensured that the study goals were followed. The coding stage was the implementation of these designs in a working system, and the advancement was marked by the successful development of the working modules that were compatible with the platform.

To measure the effectiveness, the reliability, and the usability of the platform, the testing will then be carried out. The success of the platform was gauged by its ability to carry on the functions without any errors, to attract users through the gamified features, and to increase knowledge, as evidenced by feedback from their pre- and post-assessments. Lastly, the deployment phase will be responsible for ensuring that the finished system will be delivered to the target users through proper installation, orientation, and maintenance guidelines.

Through this approach, the study will not only ensure that the CyberArena platform was conceived and developed systematically but also that its progress could be tracked at every stage and its success measured against both technical performance and user satisfaction. This method will enable a solid structure for accomplishing the platform's goal of making an engaging and accessible cybersecurity learning platform.

## Requirement Analysis

**Sampling technique.** In this study, the researchers applied the stratified sampling technique to ensure that participants from different age groups are fairly represented. The target respondents are individuals aged 15 years old and above, as they are generally more exposed to technology and capable of understanding the basic concepts of cybersecurity, making their responses more relevant and meaningful. The sampling process involves dividing the population into strata based on age groups and proportionally selecting participants from each group. This prevents the over-representation of a single age range and ensures that the data gathered reflects a balanced distribution of perspectives. Data collection will be conducted during the research phase within a set timeframe to maintain consistency in responses. The process is carried out by systematically identifying the population, categorizing them into distinct strata, and selecting respondents from each group. Through this structured approach, the researchers are able to minimize sampling bias, enhance the reliability of the data, and strengthen the overall validity of the study’s findings.

**Current Technical Situation.**

## Requirement Documentation

**Project In–Scope**

**Project Out–Scope**

## Design of Software, Systems, Product and/or Processes

## Development and Testing

**Data Analysis Plan.**

## 

## Implementation Plan

Table 5: Implementation Plan

| STRATEGY | ACTIVITIES | PERSON INVOLVED | DURATION |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |
|  |  |
|  |  |  |  |

# References

A. Thompson, L., Melendez, N., Hempson-Jones, J., & Salvi, F. (2023). View of Gamification in Cybersecurity Education: The RAD-SIM Framework for Effective Learning. [Online]. Available: <https://papers.academic-conferences.org/index.php/ecgbl/article/view/504/732>

Bitrián, P., Buil, I., Catalán, S., & Merli, D. (2024). *Gamification in workforce training: Improving employees’ self-efficacy and information security and data protection behaviours*. Journal of Business Research, 179, 114685. [Online]. Available: <https://doi.org/10.1016/j.jbusres.2024.114685>

Dhungana, R. K., Gurung Dr, L., & Poudyal, H. (2023). *Cybersecurity Challenges and Awareness of the Multi-Generational Learners in Nepal*. Journal of Cybersecurity Education, Research and Practice, 2, 5. [Online]. Available: <https://doi.org/10.32727/8.2023.17>

Fintech News Philippines. (2024, October 2). *Philippines recorded highest numbers for phishing attacks*. [Online]. Available: <https://fintechnews.ph/64749/fintech/philippines-recorded-highest-numbers-for-phishing-attacks/>

Khan, M. A., Merabet, A., Alkaabi, S., & Sayed, H. E. (2022). *Game-based learning platform to enhance cybersecurity education*. Education and Information Technologies, 27(4), 5153–5177. [Online]. Available: <https://doi.org/10.1007/s10639-021-10807-6>

Nguyen, T., Zeng, J., & Walker, L. (2020). Cooperative game-based learning in cybersecurity education: A study of teamwork and collaboration. Computers & Education, 144, 103706. [Online]. Available: <https://doi.org/10.1016/j.compedu.2019.103706>

Papamartzivanos, D., Marmol, F. G., & Kambourakis, G. (2019). Introducing a cyber training and awareness platform based on interactive gamification. Computers & Security, 87, 101600. [Online]. Available: <https://doi.org/10.1016/j.cose.2019.101600>

Peer, A., Nesher, Y., & Zohar, A. (2020). Gamification for cybersecurity education: An empirical evaluation. ACM Transactions on Computing Education (TOCE), 20(3), 1–23. [Online]. Available: <https://doi.org/10.1145/3385047>

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020). *Workforce Framework for Cybersecurity (NICE Framework)*. [Online]. Available: <https://doi.org/10.6028/nist.sp.800-181r1>

Slonopas, A. (2025, January 24). *What is cybersecurity? The realities of the digital age*. American Public University. [Online]. Available: <https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-cybersecurity-the-realities-of-the-digital-age/>

Vykopal, J., Čeleda, P., Švábenský, V., & Tovarňák, D. (2021). Scalable learning environments for teaching cybersecurity hands-on. Journal of Computer Security, 29(4), 451–472. [Online]. Available: <https://doi.org/10.3233/JCS-200046>

# 

# 

# APPENDIX A