# ENHANCING CYBERSECURITY AWARENESS AND KNOWLEDGE RETENTION THROUGH A CTF SIMULATION GAME

By

Student name: Chan Lueth Rebecca

Student number: 145843

Submitted to the School of Computing and Engineering Sciences in partial fulfillment of the requirements for the award of the Bachelor's degree in Computer Networks and Cybersecurity of Strathmore University.

School of Computing and Engineering Sciences

Strathmore University

Nairobi, Kenya.

16th July, 2024

# DECLARATION

I affirm that the project I am submitting for the Bachelor of Science in Computer Networking and Cybersecurity degree is solely my original work and has not been presented to any other higher learning institution. Additionally, I state that all sources used, referenced, or quoted within the project are properly acknowledged and indicated through a comprehensive list of references.

Admission No: 145843

Signature: ...............................................

Date: ....................................................

I confirm that this work is being submitted for examination with my approval.

Supervisor Name: Tiberius Tabulu

Signature: ...............................................

Date: ....................................................

# ABSTRACT

Cybersecurity threats have increasingly become a significant concern for organizations worldwide, necessitating innovative approaches to enhance user engagement and knowledge retention in cybersecurity awareness training. Traditional methods often fail to captivate and motivate users, leading to poor retention of critical cybersecurity practices. This study proposes a novel approach utilizing a Capture the Flag (CTF) game to gamify cybersecurity awareness training. By integrating game design elements such as puzzles, flashcards, quizzes, and narrative-driven content, the CTF game aims to create an immersive and interactive learning environment. The anticipated outcomes are improved user engagement, better retention of cybersecurity knowledge, and a proactive culture of cybersecurity within organizations. This approach addresses the human element in cybersecurity, leveraging gamification to transform passive participants into active defenders of digital security.

# LIST OF FIGURES

[Figure 2.1 Process of gamification of Cyberawareness 11](#_Toc172054264)

[Figure 2.2 Conceptual Framework 22](#_Toc172054265)

[Figure 3.1 Prototype model 24](#_Toc172054266)

# LIST OF TABLES

[Table 2.1 Related Cyberawareness Games 16](#_Toc171475213)

# LIST OF ACRONYMS

CTF - Capture the Flag

SETA - Security Education Training and Awareness

ISA - Information Security Awareness

IS - Information Systems

DDoS - Distributed Denial of Service

# TABLE OF CONTENTS

[ENHANCING CYBERSECURITY AWARENESS AND KNOWLEDGE RETENTION THROUGH A CTF SIMULATION GAME i](#_Toc172029767)

[DECLARATION ii](#_Toc172029768)

[ABSTRACT iii](#_Toc172029769)

[LIST OF FIGURES iv](#_Toc172029770)

[LIST OF TABLES v](#_Toc172029771)

[LIST OF ACRONYMS vi](#_Toc172029772)

[TABLE OF CONTENTS vii](#_Toc172029773)

[CHAPTER 1: INTRODUCTION 1](#_Toc172029774)

[1.1 Background Information 1](#_Toc172029775)

[1.2 Problem Statement 2](#_Toc172029776)

[1.3.1 General objective 3](#_Toc172029777)

[1.3.2 Specific objectives 4](#_Toc172029778)

[1.4 Research questions 4](#_Toc172029779)

[1.5 Justification 4](#_Toc172029780)

[1.6 Scope of the project 5](#_Toc172029781)

[1.7 Limitations and delimitations. 5](#_Toc172029782)

[CHAPTER 2: LITERATURE REVIEW 7](#_Toc172029783)

[2.1 Introduction 7](#_Toc172029784)

[2.2 The Human Element and Error in Cybersecurity 7](#_Toc172029785)

[2.3 Security Education, Training and Awareness (SETA) Programs 8](#_Toc172029786)

[2.3.1 Approaches to Cyber Hygiene 9](#_Toc172029787)

[2.3.2 Challenges to cyber knowledge and skills retention 9](#_Toc172029788)

[2.4 Gamification of Cyberawareness 10](#_Toc172029789)

[2.4.1 Game dynamics 12](#_Toc172029790)

[2.4.2 Game elements 13](#_Toc172029791)

[2.4.3 Game genres 14](#_Toc172029792)

[2.4 Related awareness-raising games 16](#_Toc172029793)

[2.5.1 Gaps 18](#_Toc172029794)

[2.6 Conceptual Framework 20](#_Toc172029795)

[CHAPTER THREE: METHODOLOGY 22](#_Toc172029796)

[3.1 Introduction 22](#_Toc172029797)

[3.2 System Development Methodology 22](#_Toc172029798)

[3.2.1 Requirement Analysis 23](#_Toc172029799)

[3.2.2 Design 23](#_Toc172029800)

[3.2.3 Prototyping 23](#_Toc172029801)

[3.2.4 User Evaluation 23](#_Toc172029802)

[3.2.5 Iterative Refinement 23](#_Toc172029803)

[3.3 Justification of the Methodology 24](#_Toc172029804)

[3.4 Tools and Techniques 24](#_Toc172029805)

[3.4.1 Game Development Tools 24](#_Toc172029806)

[3.4.2 Educational Content Tools 24](#_Toc172029807)

[3.5 Deliverables 24](#_Toc172029808)

[REFERENCES 26](#_Toc172029809)

[GANTT CHART 29](#_Toc172029810)

# CHAPTER 1: INTRODUCTION

## 1.1 Background Information

The modern world has become increasingly interconnected due to the proliferation of cyberspace. Cyberspace offers significant benefits to users and organizations alike, facilitating enhanced connectivity, rapid communication, information sharing, cost efficiencies, improved service delivery, entertainment options, and collaborative opportunities. However, alongside these advantages, cyberspace also introduces new threats and vulnerabilities such as malware, phishing scams, DDoS attacks, and ransomware (Mathoosoothenen et al., 2017). Organizations face heightened cybersecurity risks due to the diverse range of user access and device usage scenarios, complicating efforts to maintain robust security measures (Park et al., 2023).

To address these persistent threats and risks, there is an urgent requirement for comprehensive cybersecurity measures. These measures are designed to safeguard the confidentiality, integrity, and availability of information within computer and network systems against unauthorized access and malicious attacks (Park et al., 2023). It is a broad socio-technical topic that requires the input of people, processes, and technology to succeed. Organizations, in particular, face increased cybersecurity risks due to the diverse ways their systems are accessed by employees, customers, visitors, and third-party vendors using various devices and connecting to different services (Nagarajan et al., 2022).

While advanced security technologies and robust protocols are essential components of an organization's cybersecurity strategy, the human element is paramount. This involves educating and training employees at all levels on best practices for digital security, such as recognizing phishing attempts, creating strong passwords, and safeguarding sensitive information. Regular cybersecurity awareness programs, interactive training sessions, and simulated attacks, such as phishing tests, are employed to enhance employees' vigilance and responsiveness. By focusing on empowering individuals with the knowledge and skills to protect themselves and the organization's assets, companies can significantly reduce the risk of human error, which is often the weakest link in cybersecurity defenses. This project proposes a people-centric approach that ensures that employees are not just passive participants but active defenders in the digital security landscape, fostering a culture of cybersecurity awareness and proactive risk management.

## 1.2 Problem Statement

Cybersecurity encompasses a broad spectrum involving hardware, software, and applications, each playing a crucial role in defending against cyber threats. Hardware security focuses on safeguarding physical devices to prevent vulnerabilities that could be exploited. Software security involves developing and maintaining programs designed to withstand attacks, while application security aims to shield software applications from malicious threats throughout their entire lifecycle.

The effectiveness of cybersecurity depends on addressing vulnerabilities across hardware, software, and applications. This includes securing critical components such as the secure boot process, hardware encryption, and tamper-resistant hardware. Hardware security and software security are interconnected, often involving practices like patch management and antivirus programs. Application security, on the other hand, protects software applications through secure coding practices, application firewalls, and rigorous testing protocols.

Recent reports from 2023 indicate a troubling trend of increasing cyberattacks, with data breaches growing by over 15% annually. (Hart et al., 2020). Ransomware attacks in particular have emerged, leaving companies with the pain of financial loss and operational disturbance. This heightening threat landscape highlights the necessity for holistic cybersecurity efforts.

The human element cannot be substituted in a cyber security socio-technical system since it plays a central role. Humans are responsible for implementing the cybersecurity processes and operating the cybersecurity technology. Activities such as authentication, account management, and incident response cannot be fully automated and thus require human involvement. Therefore, effective cyber security can only be achieved by correctly applying the human element in the mitigation of cyber security threats and risks (Ashenden 2008; Boyce et al., 2011; Zimmermann & Renaud 2019).

Awareness of cybersecurity varies widely among individuals and organizations, often leading to significant vulnerabilities. Surprisingly, even professionals in the field can exhibit a lack of awareness or complacency regarding best practices. For instance, convenience often trumps security, with many people opting to save passwords in easily accessible documents, sticky notes, or allow browsers to automatically store them (Hart et al., 2020). This practice exposes them to potential breaches if their systems are compromised. This unawareness extends across various perspectives, including individual users, corporate employees, and even IT professionals, underscoring the need for comprehensive training and a cultural shift towards prioritizing security over convenience.

The central challenge lies in the low levels of engagement and retention observed in traditional cyber awareness training programs. These programs often lack dynamism and fail to capture the interest of users, resulting in a lack of motivation to learn and apply cybersecurity best practices. Users, identified as the weakest link in cybersecurity socio-technical systems, are more susceptible to manipulation compared to technology (Hart et al., 2020). Despite their critical role, users have traditionally received inadequate attention in cybersecurity initiatives. This deficiency in effective cyber awareness training adversely affects employees, organizations, and society as a whole. Employees become more vulnerable to cyber-attacks, organizations face heightened cybersecurity risks and potential financial repercussions, and society at large suffers from the pervasive impacts of data breaches and cybercrime.

Various strategies have been employed to enhance cyber awareness, such as interactive e-learning modules, phishing simulation exercises, and workshops. However, these approaches often lack the immersive and captivating qualities necessary to sustain user engagement. Gamification, which integrates game design elements into non-game contexts, presents a promising solution by enhancing user involvement and motivation (Hart et al., 2020). It has been advocated by researchers and experts as a means to render cyber awareness training more stimulating, yet comprehensive studies on its effectiveness and optimal implementation strategies remain limited.

This project proposes the development of a series of Capture the Flag (CTF) games featuring puzzles, flashcards, quizzes, and narrative-driven content aimed at promoting active learning. The goal is to establish an immersive learning environment where users can actively engage in tackling cybersecurity challenges, thereby fostering enhanced retention of knowledge and practical skills in an enjoyable and interactive manner.1.3 Objectives

### 1.3.1 General objective

This project introduces gamification in training, enhancing user engagement and knowledge retention in cyber awareness programs by creating a capture the flag (CTF) game to keep users engaged while actively learning.

### 1.3.2 Specific objectives

1. To identify and assess challenges in knowledge retention within traditional cyber awareness training, pinpointing gaps in current methods.
2. To review and evaluate existing research on game theory in cybersecurity education to extract insights and best practices for similar awareness games.
3. To design and conceptualize a series of Capture the Flag (CTF) games tailored for cybersecurity awareness, emphasizing user engagement and knowledge retention.
4. To develop and implement the designed CTF games for cyber awareness training, ensuring they are interactive and educational.
5. To test and evaluate the CTF games in real-world scenarios to gauge their effectiveness in enhancing user engagement and knowledge retention compared to traditional training methods.Top of Form

Bottom of Form

## 1.4 Research questions

1. What are the key challenges and limitations in knowledge retention observed in traditional cyber awareness training programs?
2. How can game theory be effectively applied in cybersecurity education to enhance awareness and knowledge retention?
3. What are the optimal design principles for developing Capture the Flag (CTF) games that promote engagement and improve cybersecurity awareness?
4. How can interactive and educational elements be integrated into the development of CTF games for effective cyber awareness training?
5. What is the comparative effectiveness of CTF games versus traditional training methods in improving user engagement and knowledge retention in real-world cybersecurity scenarios?

## 1.5 Justification

The justification for this project lies in addressing the critical need for effective cybersecurity awareness training amidst increasingly sophisticated cyber threats. Traditional methods often fail to engage users and ensure lasting knowledge retention. This project proposes a gamified training program through a Capture the Flag (CTF) simulation game to enhance user engagement and retention by transforming training into an interactive and enjoyable experience. Gamification incorporates elements of play, competition, and rewards, making training more appealing and effective. Interactive learning methods, such as CTF games, provide practical, hands-on scenarios that improve knowledge retention and real-world application. By focusing on engaging and educating users, this project aims to mitigate the risk of human error, fostering a proactive cybersecurity culture within organizations. It also offers the flexibility to develop customized training programs tailored to specific organizational needs, ensuring relevance and applicability. Investing in such a program can lead to long-term cost savings by reducing the likelihood of costly data breaches and supporting organizational goals of protecting sensitive information, maintaining customer trust, and ensuring regulatory compliance.

## 1.6 Scope of the project

This project comprises of the development, designing and evaluating the Capture the Flag (CTF) simulation games so as to increase user involvement and knowledge retention while in cybersecurity awareness training in organizations. The project’s focus is with mobile app-based CTF games that will be utilized for interactive, gamified experiences to educate employees about best practices on how to secure their information technology systems. The main activities include examining problems and constraints of traditional cyber awareness programs, constructing CTF games, and studying their efficacy under real-life circumstances respectively. Besides, we will nonetheless evaluate users’ feedbacks through which game would be continuously improved in terms of education objectives so as to boost engagement rate among players. In conclusion, it aims at supplying a realistic and enjoyable approach to computer protection that prevents human errors and reinforces organizational safety measures.

## 1.7 Limitations and delimitations.

The execution of this project is expected to encounter several limitations and delimitations. Technological constraints may pose challenges, particularly in ensuring compatibility across various devices and platforms, which could require additional time and investment than what is currently available. User engagement variability is another limitation, as the gamified approach may not equally appeal to all individuals, given their varied preferences and motivations. Scalability issues might arise when implementing the CTF game across large organizations, making it difficult to maintain consistent performance and user experience. Additionally, there are inherent security concerns, as simulating attacks in a training context must be carefully controlled to avoid inadvertent harm. The project is also resource-intensive, demanding significant time, expertise, and financial investment, potentially facing budgetary, and constraints.

The project's scope is delimited to focus on developing a gamified training program that is only focused on cybersecurity awareness, excluding all other training or educational content. It will be delivered via mobile applications, not exploring other platforms such as desktop or web-based solutions. The primary target audience is employees within organizational settings, excluding other potential user groups like individual consumers or students. The training content will cover key cybersecurity concepts and best practices relevant to organizational security, without delving into advanced technical topics that require specialized knowledge. The effectiveness of the CTF game will be evaluated over a defined period, concentrating on immediate and short-term impacts on user engagement and knowledge retention, without assessing long-term effects or continued engagement post-implementation. By acknowledging these limitations and delimitations, the project aims to deliver a targeted, practical, and impactful cybersecurity training solution while being mindful of the potential challenges and constraints it may face.

# CHAPTER 2: LITERATURE REVIEW

## 2.1 Introduction

This chapter covers cyber Security, Education, Training, and Awareness (SETA) as well as the human element. It focuses on the importance of cyber hygiene within organizational cybersecurity frameworks, and the main practices to ensure it, and also examines the delicate role of the human factor for every organization’s cybersecurity posture. The chapter also discusses innovative approaches like gamification in security awareness training, aiming to enhance engagement and effectiveness in educating users about cybersecurity risks and best practices as well as improving their knowledge and skill retention. Top of FormBottom of Form

## 2.2 The Human Element and Error in Cybersecurity

Human error is the leading cause of security risks and breaches in several organizations which points to humans as the weakest link in cybersecurity (Hart et al., 2020). The human element in cybersecurity is basically the potential risks that arise from human activity (Zoto et al. 2018). Effective cybersecurity depends on socio-technical systems that recognize the interaction between people and technology. These systems involve complex interactions among social, psychological, technical, and environmental components, which must work together for the system to function efficiently.

The technical component is made up of machinery and methods, while the socio component encompasses structure and culture. Structure refers to a user's position within an organization (management or support staff), and culture involves values and traditions. The human element is influenced by differences in characteristics, personalities, and behavior, which affect cybersecurity attitudes, beliefs, values, traditions, and threat perceptions (Khan et al., 2021). Factors such as age, gender, citizenship, personality traits, risk-taking, and decision-making also impact the human element in cybersecurity.

Humans are central to cybersecurity socio-technical systems, responsible for implementing processes and operating technology. Activities like authentication, account management, and incident response require human involvement. Therefore, effective cybersecurity relies on correctly applying the human element to mitigate threats and risks. Despite their crucial role, humans are considered the weakest link due to a lack of awareness, poor practices, lack of shared responsibility, low motivation, and non-user-friendly practices. This vulnerability leads to threats like privilege escalation, social engineering, unauthorized access, denial of service, identity theft, phishing, and ransomware (Kadena & Gupi, 2021).

Human behavior's unpredictability and irrationality can compromise cybersecurity. Pinpointing human error in incidents is challenging due to the complexity of socio-technical systems. Therefore, while humans are often seen as the weakest link, their role in creating or mitigating risks must be properly understood. The human element should be viewed as a solution rather than a problem in cybersecurity.

The success or failure of cybersecurity in an organization depends on its users. Prioritizing user management through security awareness helps minimize human error by educating users on the value of information and information risks. Targeted security awareness can change the cybersecurity behavior of a few users, leading to overall behavioral change within the organization, as users tend to align with their peers. By addressing knowledge gaps and providing proper technical support, the human element becomes a solution t ensuring cybersecurity.

## 2.3 Security Education, Training and Awareness (SETA) Programs

Users now have widespread access to critical organizational information through ubiquitous, enterprise-wide systems. While these systems enhance operational efficiency and effectiveness, they also amplify the organization's exposure to risk. Organizations face increasing vulnerability due to user actions, underscoring the importance of managing user behavior. To address this, organizations implement cybersecurity policies, procedures, and security awareness training. A cybersecurity policy establishes standards, rules, and practices that govern user conduct within the organization. It covers activities such as email usage, social media interactions, password management, remote access protocols, and information encryption. These policies primarily focus on prohibiting detrimental cybersecurity behaviors rather than instructing users on positive actions (Koohang et al., 2020).

Security awareness, conducted through Security Education, Training, and Awareness (SETA) programs, plays a critical role in safeguarding the organization's sensitive information, often referred to as its "crown jewels." SETA programs are educational initiatives designed to reduce cybersecurity breaches by enhancing user awareness across the organization. They are tailored to educate all users about the organization's cybersecurity policies and define cybersecurity standards based on their respective roles. Effective SETA programs not only inform users about policies but also explain the rationale behind them. Tailoring SETA programs to align with the unique cybersecurity needs of users and the organization is crucial for their effectiveness. A well-executed SETA program alerts users to cybersecurity threats, thereby fostering greater awareness and encouraging responsible cybersecurity practices (Hu et al., 2022).

### 2.3.1 Approaches to Cyber Hygiene

Cyber hygiene encompasses practices that promote the maintenance of system health and security, reducing vulnerabilities and enhancing resilience against cyber threats. Fundamental cyber hygiene practices include regular software updates and patch management to address known vulnerabilities promptly. These updates fix security flaws identified by developers and researchers, minimizing the risk of exploitation by malicious actors. Strong password management policies are essential to safeguarding access to systems and accounts. Implementing complex password requirements, enforcing regular password changes, and promoting the use of password managers enhance overall security posture. Additionally, educating users about phishing threats and social engineering tactics reduces the likelihood of falling victim to fraudulent schemes aimed at obtaining sensitive information.

Network segmentation and segregation isolate critical assets and sensitive data, limiting the impact of potential breaches and containing malicious activities within restricted areas. By segmenting networks based on user roles and data sensitivity levels, organizations bolster their defense-in-depth strategies and mitigate lateral movement by attackers. Continuous monitoring of network traffic and endpoint devices enables early detection of anomalies and potential security incidents. By leveraging security information and event management (SIEM) systems and endpoint detection and response (EDR) solutions, organizations gain real-time visibility into their IT environments, facilitating proactive threat detection and incident response efforts.

### 2.3.2 **Challenges to cyber knowledge and skills retention**

In the realm of cybersecurity, maintaining and advancing knowledge and skills poses significant challenges due to the rapid evolution of threats and technologies. One primary obstacle is the constant need for professionals to stay updated with the latest trends in cyber threats, which often outpace traditional educational curricula. Additionally, the interdisciplinary nature of cybersecurity demands expertise in fields ranging from computer science to law and psychology, making it difficult to keep a comprehensive skill set current.

Another critical challenge is the high turnover rate within the cybersecurity workforce, leading to knowledge loss and skill gaps within organizations. This turnover can stem from competitive job markets, burnout due to the intense nature of the work, or inadequate professional development opportunities. Consequently, organizations struggle to retain institutional knowledge and experience, hindering their ability to adapt swiftly to new threats.

Moreover, the dynamic nature of cybersecurity necessitates continuous learning and adaptation, which traditional training methods may not adequately address. As technologies evolve, new vulnerabilities emerge, requiring cybersecurity professionals to possess not only technical skills but also analytical and strategic thinking abilities. Overcoming these challenges requires innovative approaches to training and development, such as hands-on simulations, gamification of learning processes, and ongoing mentorship programs to foster skill retention and career longevity in the cybersecurity field.

## 2.4 Gamification of Cyberawareness

Gamification is continuously being used in education to better learning outcomes in a fun way. It has introduced a revolution education-wise with player engagement being a huge priority. This same thing can be applied in security awareness to improve knowledge and skill retention by seamlessly blending entertainment, competition, and learning gamification can increase enthusiasm during security awareness training. Gamification takes advantage of the addictive nature of the human brain to create enthusiasm and motivation lacking in current security awareness training (Kadena & Gupi, 2021).

Gamification is the integration of game mechanics and elements into non-game contexts to enhance engagement and user experience. It involves employing concepts such as rewards, feedback systems, progress tracking, collaborative activities, problem-solving challenges, narrative elements, and competitive elements to motivate participation and promote desired behaviors. (Hart et al., 2020). It involves employing concepts such as rewards, feedback systems, progress tracking, collaborative activities, problem-solving challenges, narrative elements, and competitive elements to motivate participation and promote desired behaviors (Koohang et al., 2020).

Gamification of security awareness is the use of game concepts during security awareness training to increase player motivation and engagement. The process of gamification is shown in Figure 2.1 below. There is a difference between gamifying content and the gamification method. Gamifying content converts security awareness content into a story or animation. This conversion makes the content more descriptive, explanatory, and also introduces an entertaining element. However, there is a risk that in the process of gamifying content the converted content becomes unrecognizable to the player. As a result, the security awareness training objectives are missed. In gamification the security awareness content remains the same, the difference being the introduction of game elements to the content (Koohang et al., 2020).

A game is an artificial system in which players follow provided rules to achieve set objectives or overcome obstacles. Games provide players with a virtual environment that is similar to their real-world environment. They use these virtual environments to practice, get hands-on experience, and explore the consequences of their actions. The best way to learn and understand is through trial and error. By practicing in a virtual environment players can learn, improve, and reinforce good cyber security behavior.

Games also satisfy other requirements such as skill-building, mastery, socializing, and prestige. There are a lot of benefits to be gained from gamification if it is applied to the right players and in the correct context. The use of games in learning is referred to as game-based learning. Game-based learning has been used in education, health, advertising, and behavioral science. Serious games are games that have a purpose besides entertainment. Serious games are used to promote learning and behavioral change (Hart et al., 2020).

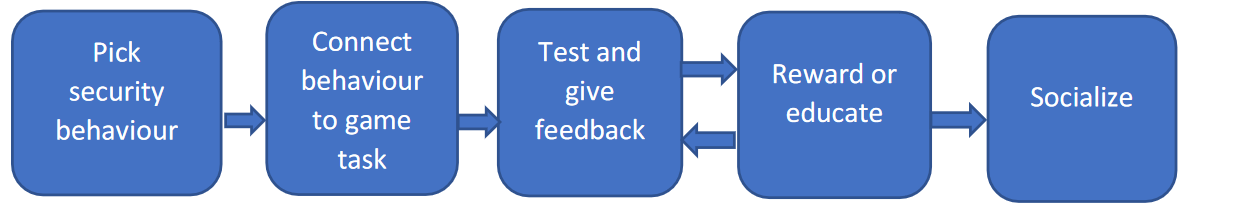


Figure 2.0.1 Process of gamification of Cyberawareness

Some suggested steps for implementing gamification in security awareness training are as follows (Armstrong & Landers 2018): Firstly, set training goals by identifying knowledge and performance gaps. Secondly, develop a game incorporating appropriate design elements and instructional practices. Thirdly, conduct training using the game and collect data for evaluation. Lastly, refine the game based on feedback until desired outcomes are achieved. Customization enhances relevance and understanding. Gamification aims to increase motivation by engaging players in practical applications and providing continuous feedback on progress.

### 2.4.1 Game dynamics

Game dynamics encompass the evolving patterns that shape gameplay and motivate players to continue engaging with a game. Player motivations vary widely, from competitiveness to collaboration, and game dynamics are tailored to address these diverse preferences. Below are several game dynamics identified by Nagarajan et al. (2012), along with their applications in security awareness games:

1. Territorial Acquisition Dynamic: This dynamic revolves around the acquisition of limited resources, encouraging players to strategically control them. In security awareness games, players might focus on acquiring and managing resources like network bandwidth, computer memory, or servers to strengthen their defenses.
2. Prediction Dynamic: Players engage in predicting future events and are rewarded for accurate predictions. In security awareness games, players could earn rewards for correctly identifying the source of cyber-attacks or predicting upcoming security breaches.
3. Spatial Reasoning Dynamics: This involves solving puzzles or spatial challenges. In security awareness games, players might utilize spatial reasoning to develop intricate cybersecurity strategies, such as creating defense-in-depth architectures to protect sensitive data.
4. Survival Dynamic: Based on human instinct for self-preservation, this dynamic centers on life-and-death challenges. In security awareness games, players might safeguard critical systems or servers from cyber-attacks, simulating real-life scenarios where swift action is essential to prevent system compromise.
5. Destruction Dynamic: This dynamic focuses on eliminating threats or obstacles. In security awareness games, players may be tasked with removing viruses, malware, or intruders from a network environment to ensure system integrity and data protection.
6. Building Dynamic: Players engage in constructing or enhancing aspects of the game environment. In security awareness games, this could involve building secure networks, improving cybersecurity protocols, or enhancing personal defenses against online threats.
7. Chasing and Evading Dynamic: This dynamic involves pursuit or evasion tactics. In security awareness games, players might assume roles such as hackers evading detection while infiltrating networks or defenders tracking down and neutralizing cyber threats.
8. Trading Dynamics: Inspired by tabletop games, this dynamic includes negotiation and resource exchange. In security awareness games, players may trade cybersecurity resources, make strategic decisions on resource allocation, or negotiate collaborative efforts to strengthen overall defences.
9. Race-to-the-End Dynamics: This dynamic fosters competition to achieve objectives quickly. In security awareness games, players may compete to be the first to secure a network, implement critical security updates, or mitigate emerging threats to maintain system resilience.

### 2.4.2 Game elements

Game elements are defined as the components that make up a game. It is also referred to as game attributes. Game elements make security awareness games enjoyable while maintaining their learning aspects. The target audience and the game’s intervention purpose determine the game elements used. The game elements essential in security awareness games (Hu et al., 2022):

i. Conflict in games involves tasks that players must overcome, whether it's tackling obstacles, competing with others, or solving puzzles. It can also include cooperative challenges that require teamwork. Incorporating cyber security conflicts into games helps players develop skills and knowledge to handle similar real-life situations effectively.

ii. Strategy and variability are integral to games, where players' decisions influence outcomes and their ability to achieve objectives. Random elements add uncertainty and excitement. Security awareness games should blend strategic decision-making with unpredictable challenges to engage players effectively.

iii. Aesthetics play a role in attracting players by creating visually appealing environments that immerse them in the game. While aesthetics are less crucial in security awareness games, they still contribute to engagement and should not be overlooked.

iv. Themes and stories provide context and connection for players, enhancing their engagement and memory retention. Narratives within games make information more memorable compared to isolated facts.

v. Rewards in games signify achievements and motivate players. In security awareness games, rewards like points and badges should be tied to completing tasks according to proficiency standards, providing effective feedback and encouraging continued engagement.

vi. Mystery in games motivates players to seek information and solve gaps between known and unknown elements. In security awareness games, this could involve locating critical cybersecurity policies, akin to uncovering a hidden key to progress.

vii. Challenge drives player engagement by stimulating critical thinking and problem-solving skills. Security awareness games should continually challenge players to promote active learning and skill development.

viii. Penalties in games enforce consequences for incorrect actions, encouraging players to pay attention and learn from mistakes. In security awareness games, penalties simulate real-world consequences of cybersecurity errors, fostering awareness and caution.

ix. Mastery opportunities in games allow players to progress and demonstrate their expertise. Advancing through increasingly difficult levels as they master skills keeps players motivated and engaged in security awareness games.

x. Progress visibility in games provides ongoing feedback on performance, such as progress bars or module updates. In security awareness games, clear and timely progress indicators help players track their learning journey and stay motivated.

xi. Emotional engagement in games evokes a range of human emotions like excitement, frustration, and joy, enhancing learning and memory retention. Security awareness games should harness these emotions to create impactful learning experiences that resonate with players.

### 2.4.3 Game genres

Game genres categorize games based on their type or style, offering both game designers and players insights into the game's nature and the skills required to engage with it. Security awareness games often incorporate a variety of genres to enhance engagement and effectiveness. Here are several game genres and their applications in security awareness games:

i. Action Genre: These games provide intense, adrenaline-fueled experiences that demand quick reflexes and decisive actions under pressure. Examples include tower defense games where players protect against cyber-attacks, requiring swift decision-making to safeguard digital assets.

ii. Role-playing Genre: In these games, players assume fictional character roles within a defined setting, making decisions and strategizing based on their character's traits and objectives. Role-playing games (RPGs) often feature rich storylines and character progression, reflecting scenarios where players take on roles like system administrators defending servers or hackers infiltrating systems for specific objectives.

iii. Simulation Genre: Simulation games replicate real-world activities or scenarios, using models to represent systems or processes. In cybersecurity, these games simulate network environments with realistic cyber threats and activities. Players engage in defending or attacking these simulated networks, honing their cybersecurity skills in controlled environments.

iv. Adventure Genre: Known for exploration and puzzle-solving, adventure games challenge players to unravel storylines and overcome obstacles. In security awareness games, they can simulate disaster recovery scenarios post-security breaches, where players solve puzzles to mitigate and recover from cyber incidents.

v. Sports Genre: These games emphasize team collaboration and role specialization, where each member contributes to achieving a shared objective. Applied in security awareness games, the sports genre can simulate team-based responses to cyber-attacks, training players in coordinated defense strategies and roles within a cybersecurity incident response team.

vi. Casual Genre: Characterized by simplicity and accessibility, casual games are easy to learn and typically start afresh in each session. They can introduce players to basic cybersecurity concepts, terminology, and techniques in an engaging manner, making them suitable for initial cybersecurity training and familiarization.

vii. Capture the Flag (CTF) Genre: CTF games pit players or teams against each other in cybersecurity challenges. Variants include attack-defend CTF, where players both attack opponents and defend their own assets, and jeopardy CTF, where players solve puzzles to capture flags representing success in cybersecurity tasks. These games are timed and promote competitive problem-solving skills in real-time cyber scenarios.

## 2.4 Related awareness-raising games

Table 2.1 Related Cyberawareness Games

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Game name | Cyber security topic | Game genre | Target  audience | Deployment  method | Reference |
| Control-Alt-Hack | Botnets  Unpatched software  Insider threat  Social engineering  Tracking | Role-playing | Students | Card game | (Hart, 2022) |
| Project config.  play | Authentication  requirements  and  exposure (CVE) | Turn-based  strategy | General  Public | Boardgame  Card game | (Ciussi, 2018) |
| Cyber CIEGE | Cyber security  definitions  Social engineering  Malware  Data protection  Physical security | Role-playing | Employees | Computer  game | (Hart, 2022) |
| Network  nightmares | Viruses  Network monitoring  Port vulnerabilities | Shooter | General  Public | Computer  game | (Kadena & Gupi, 2021) |
| M-learning | Passwords  Phishing  Malware  Data protection | Quiz  Survival | Employees | Android  Mobile application  game | Filipczuk et al.,  (2019) |
| Integrated ethical  hacking  toolkit | Screen and keyboard  capture  Ransomware | Simulation  Quiz | General  Public | Computer  game | Mathoosoothenen et  al., (2017) |
| Hacked time | Data breach  Cyber security threats  identification | Puzzle  Role-playing  Interactive  narrative  Tower defence | General  Public | Computer  game | Chen et al., (2020);  Chen et al., (2019) |
| Cyber smart | Firewall  Safe web surfing Security software  Secure wireless  connection  Passwords | Role-playing | Students | Computer  game | Underhay et al.,  (2016) |
| Cyber security  requirements  awareness game | Network security  Physical security  Social engineering | Narrative  Role-playing  Puzzle | Employee  Students | A board  game that  uses a floor  map  Cards | Yasin et al., (2018) |
| Secu-one | Cyber security threat  analysis  Cyber security | Turn-based  strategy | Students  Employees | Card game | Omiya &  Kadobayashi (2019) |
| Cyber Agents’  Interactive  Modelling and  Simulation  (CyberAIMs) | Factors that affect  cyber security  motivation and  incentives | Simulation | Students | Computer  game | Zoto et al., (2018) |
| Internet Hero | Emails  Malware  Social networks  Internet connection | Fiction  Interactive  narrative | Children | Computer  games | Bauer et al., (2013) |
| Educational  games for cyber  security | Laptop security  Social networks  Malware  Smart Internet usage | Quiz Shooter  Endless runner | Students  Children | Card  matching  game  Computer  game | Sookhanaphibarn &  Choensawat (2020) |
| Escape room | A clean desk and  screen policy  Social networks  Shredding | Simulation  Role-playing | Employees | Escape room | Oroszi (2019) |
| Security Empire | Software patching  Passwords  Anti-virus | Role-playing | General  public | Computer  game | Olano et al., (2014) |
| Cyber VR | Data privacy  Access privileges  Cryptography | Role-playing Fiction  Interactive  narrative | General  public | Virtual reality  game  Computer  game | Veneruso et al.,  (2020) |
| CybAR | Bad cyber security  behavior to avoid | Role-playing  Quiz | General  public | Augmented  Reality  Android  mobile  application  game | (*The Impact of Gamification in Educational Settings on Student Learning Outcomes: A Meta-Analysis | Educational Technology Research and Development*, n.d.) |
| 3D Virtual reality  (VR) game | Social engineering  e.g. piggybacking,  mantrap, and  tailgating  Ransomware  Distributed denial of  service | Role-playing  Simulation Strategy  Tower defence | Students | Cards  Virtual reality  game  Computer  game | Jin et al., (2018) |
| CyberNEXS | Cyber defence  Penetration testing  Cyber forensic | Simulation | Students | Computer  game | Nagarajan et al.,  (2012) |
| Capture the Flag  (CTF) | Cyber security  terminology  Cyber defence  Vulnerability exploitation  Network configuration  Network vulnerabilities  Phishing | CTF scavenger  hunt  CTF king of the  castle Quiz  Turn-based  Strategy | Students | Computer  game | Leune & Petrilli  (2017) |
| Class Capture the  Flag (CCTF) | Cryptography  Intrusion  Denial of Service  Domain name system  (DNS) security | Role-playing  Capture the Flag Turn-based  Strategy | Students | Computer  game | (*Cybersecurity Awareness and Market Valuations - ScienceDirect*, n.d.) |
| Hardware CTF | Hardware  Trojans  Unprotected test  infrastructure | Quiz  Capture the Flag  Turn-based  Strategy | General  public | Digital  hardware  design  representatio  n  Physical  hardware  devices  Electronic  device  automation  tool | Prinetto et al., (2020) |

### 2.5.1 Gaps

1. **Educational Depth and Breadth:**

While many games cover specific topics like malware, social engineering, and network vulnerabilities, there is a potential for enhancing the depth and breadth of educational content. Ensuring comprehensive coverage of these topics with detailed explanations and practical examples could improve learning outcomes.

1. **Target Audience Alignment:**

Although some games specify their target audience (e.g., students, the general public, employees), ensuring that the content, difficulty level, and teaching approach align well with the knowledge and experience of the intended users could enhance engagement and effectiveness.

1. **Interactive Learning Features:**

Many games incorporate quizzes, simulations, or role-playing elements, but there is room to introduce more interactive and adaptive learning features. Personalized learning paths, feedback mechanisms, and adaptive difficulty settings could cater to diverse learning styles and improve user engagement.

1. **Real-World Application Integration:**

Enhancing the integration of real-world cybersecurity scenarios and practical applications within the games could provide more relevant and applicable learning experiences. This could help users bridge the gap between theoretical knowledge and practical skills.

1. **Accessibility and Platform Compatibility:**

Considering accessibility across different platforms (mobile, PC, VR) and ensuring compatibility with various devices could broaden the reach and usability of these educational games. This inclusivity could make cybersecurity education more accessible to a wider audience.

1. **Timely Updates and Relevance:**

Given the fast-paced nature of cyber threats and technology advancements, regular updates to game content to reflect current trends and challenges in cyber security would ensure ongoing relevance and engagement. This could keep the educational content up-to-date and aligned with industry developments.

1. **Feedback and Assessment Mechanisms:**

Implementing robust feedback and assessment mechanisms within the games could provide users with clear insights into their progress and areas needing improvement. This could enhance learning outcomes by facilitating self-assessment and continuous learning.

1. **Collaborative and Competitive Elements:**

Expanding collaborative and competitive features within the games, such as team challenges or multiplayer modes, could foster peer learning, teamwork, and healthy competition among users. This could enhance engagement and motivation to learn cybersecurity concepts.

## 2.6 Conceptual Framework

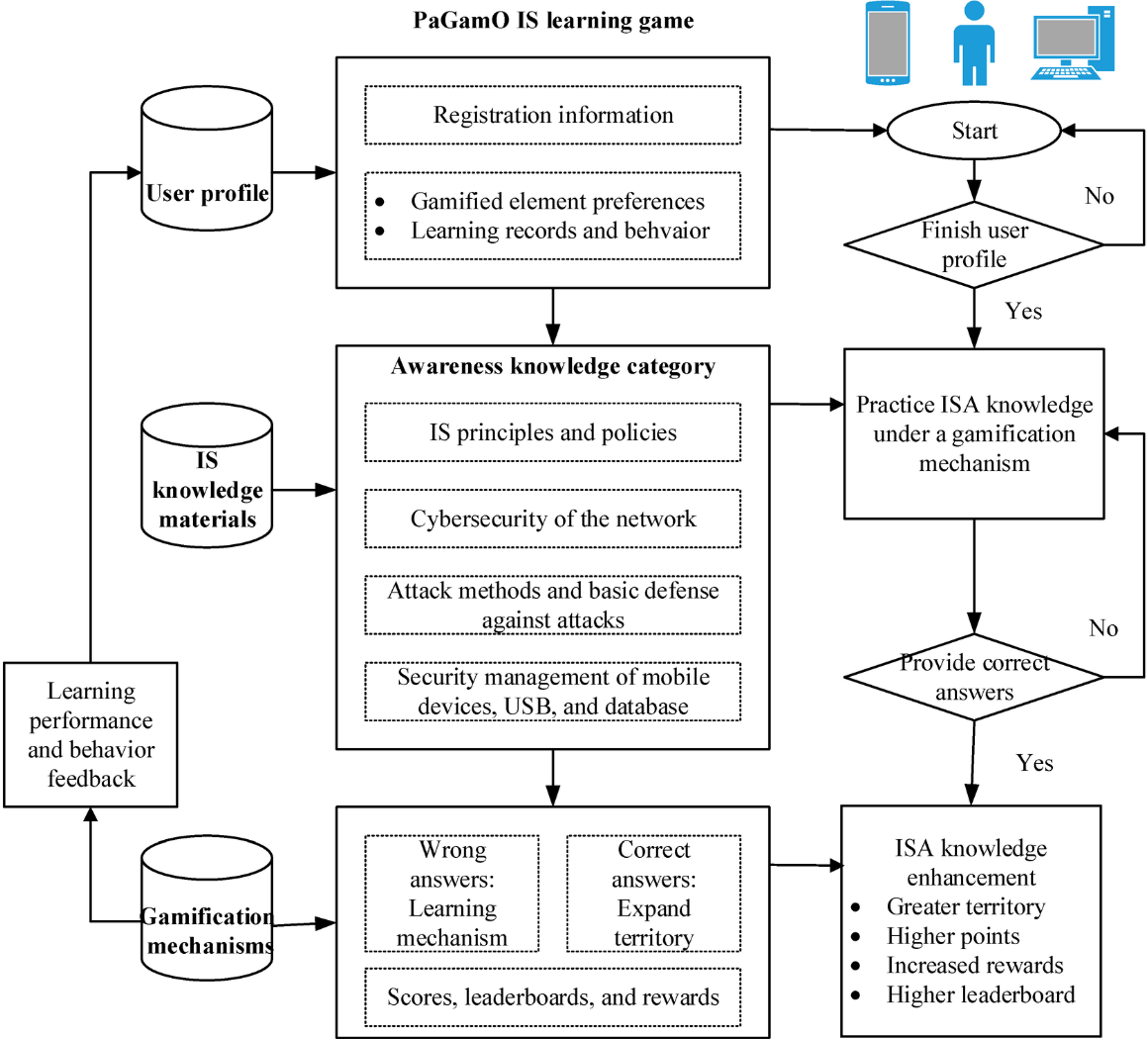


Figure 0.2 Conceptual Framework

The system operates through a mobile-based IS digital game designed to foster an understanding of ISA concepts using gamification techniques. It features a user-friendly interface accessible on mobile devices, aiming to minimize technical obstacles that might impede learning while ensuring broad availability.

Key components of the game system include:

1. **User’s Profile Database:** This repository stores registration details and monitors user performance and behavior patterns over time.
2. **IS Knowledge and Materials Database:** This database houses a comprehensive collection of IS learning materials categorized into awareness, technical skills, and management topics.
3. **Gamification Mechanisms Database:** Here, various game dynamics such as points, leaderboards, rewards, and tools are integrated to enhance user engagement and motivation.

Within the game environment, users register and personalize avatars before participating in individual or collaborative gaming tasks. They apply ISA knowledge through interactive game-based mechanisms, earning scores by correctly answering questions to expand their influence within the game. Incorrect responses trigger learning mechanisms designed to facilitate improvement.

To boost engagement and motivation, the system employs diverse gamification elements including point accumulation, real-time leaderboard standings, and rewards for achievements. This approach not only encourages active learning but also creates an immersive experience that enhances the retention and application of ISA knowledge in practical scenarios.

# CHAPTER THREE: METHODOLOGY

## 3.1 Introduction

This chapter outlines the methodology used in the development of a gamified cyber awareness game aimed at educating users in an engaging manner. It discusses the system requirements, development tools, and techniques employed to achieve the project's educational objectives effectively.

## 3.2 System Development Methodology

The methodology selected for developing the gamified cyber awareness game is the Prototyping approach. Prototyping involves iterative development of early versions of the game to gather user feedback, identify potential issues, and refine the game design. This iterative process ensures that the final game meets user expectations and effectively enhances cyber awareness through interactive gameplay.

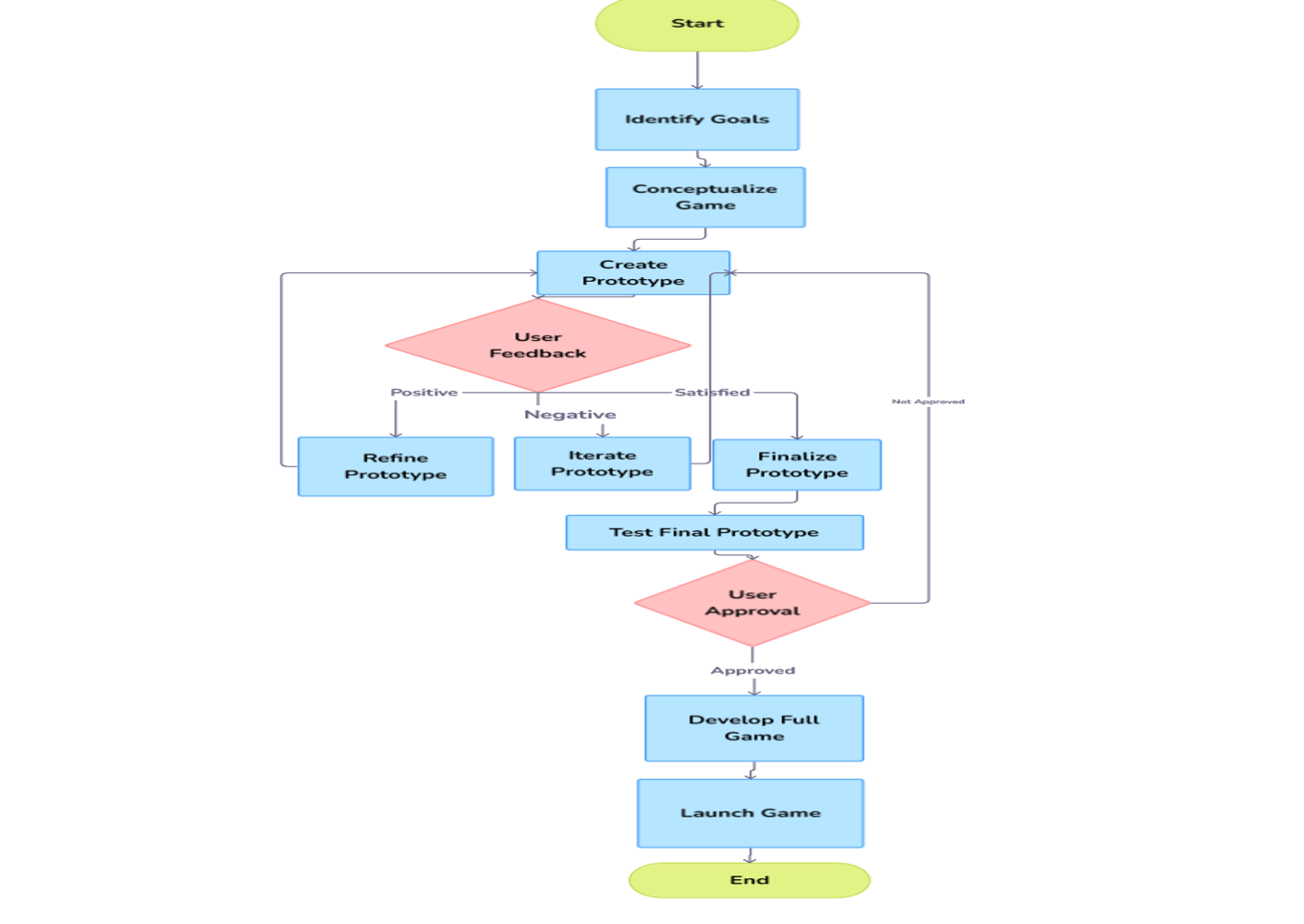


Figure 3.1 Prototype model

### 3.2.1 Requirement Analysis

Initially, requirements for the gamified cyber awareness game are gathered and analyzed. This process includes conducting research through a literature review and consultations with stakeholders such as cybersecurity experts and potential users. Key game mechanics, educational content, and cybersecurity learning objectives are identified during this phase to guide subsequent design and development activities.

### 3.2.2 Design

The design phase focuses on creating both conceptual and technical designs for the cyber awareness game. This includes defining the game's architecture, user interface design, interactive elements (e.g., scenarios, quizzes), and integration of gamification mechanics (e.g., points, leaderboards). The design phase lays the groundwork for implementing an engaging and educational game environment.

### 3.2.3 Prototyping

Prototyping involves the iterative development of the gamified cyber awareness game. Initial prototypes are created to demonstrate core functionalities, user interactions, and educational content. These prototypes are tested and refined based on user feedback, ensuring that the game remains aligned with educational objectives and enhances user engagement through interactive learning experiences.

### 3.2.4 User Evaluation

Throughout the development process, prototypes of the game are evaluated by target users to assess usability, functionality, and educational effectiveness. User testing provides valuable insights into the game's strengths and areas for improvement, guiding iterative refinements to enhance overall user experience and learning outcomes.

### 3.2.5 Iterative Refinement

The iterative refinement process focuses on continuously improving the game based on feedback from user evaluations and emerging trends in cybersecurity education. This iterative approach allows for adjustments to game mechanics, content updates, and enhancements to ensure the game remains relevant and impactful in raising cyber awareness among its users.

## 3.3 Justification of the Methodology

The Prototyping methodology is justified for its ability to facilitate early validation of game concepts, incorporate user feedback, and adapt to evolving educational needs and cybersecurity challenges. By iterating on prototypes, the game development process minimizes risks and ensures that the final product effectively meets user expectations while promoting active learning and engagement.

## 3.4 Tools and Techniques

### 3.4.1 Game Development Tools

1. Unity3D: Cross-platform game engine for developing interactive 3D and 2D games, providing robust features for graphics, physics, and user interface design.
2. C#: Programming language integrated with Unity3D for scripting game logic and interactions.
3. Kotlin: Programming language used and integrated with Unit3D to create a Mobile Application game.

### 3.4.2 Educational Content Tools

1. Articulate Storyline: E-learning authoring software for creating interactive educational content within the game.
2. Adobe Creative Suite: Design tools for developing visual assets, animations, and user interface elements.

## 3.5 Deliverables

The development of the gamified cyber awareness game will produce several key deliverables aimed at creating an engaging and effective educational experience that enhances users' understanding of cybersecurity concepts.

1. **Iterative Prototypes**: These prototypes will demonstrate core game mechanics, interactive scenarios, and gamification elements like points and leaderboards. Each iteration will refine and enhance these aspects based on testing and feedback.
2. **Comprehensive Design Documentation**: This documentation will outline the game's architecture, including how different components interact and support the game's objectives. It will also detail user interface designs, ensuring they are intuitive and supportive of the gameplay experience. Additionally, it will describe how educational content on cybersecurity is integrated into the game to align with learning objectives.
3. **User Evaluation Reports**: Reports generated from iterative testing phases will provide valuable insights into gameplay, user engagement, and educational effectiveness. These reports will guide further development and refinement of the game to enhance its usability and educational impact.
4. **Fully Functional Game**: The final deliverable will be a fully functional version of the gamified cyber awareness game. This version will be optimized for usability across multiple platforms and will effectively convey cybersecurity concepts in an immersive and dynamic learning environment.

# REFERENCES

Ciussi, D. M. (2018). *ECGBL 2018 12th European Conference on Game-Based Learning*. Academic Conferences and Publishing Limited.

*Cybersecurity awareness and market valuations—ScienceDirect*. (n.d.). Retrieved July 2, 2024, from https://www.sciencedirect.com/science/article/abs/pii/S0278425418302370

Hart, S. (2022). *A pedagogical design model to create serious games for cyber security* [Phd, University of Southampton]. https://eprints.soton.ac.uk/457783/

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*, *95*, 101827. https://doi.org/10.1016/j.cose.2020.101827

Hu, S., Hsu, C., & Zhou, Z. (2022). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, *62*(4), 752–764. https://doi.org/10.1080/08874417.2021.1913671

Kadena, E., & Gupi, M. (2021). HUMAN FACTORS IN CYBERSECURITY: RISKS AND IMPACTS. *Security Science Journal*, *2*(2), Article 2.

Khan, N. F., Ikram, N., Murtaza, H., & Asadi, M. A. (2021). Social media users and cybersecurity awareness: Predicting self-disclosure using a hybrid artificial intelligence approach. *Kybernetes*, *52*(1), 401–421. https://doi.org/10.1108/K-05-2021-0377

Koohang, A., Anderson, J., Nord, J. H., & Paliszkiewicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, *120*(1), 231–247. https://doi.org/10.1108/IMDS-07-2019-0412

Mathoosoothenen, V. N., Sundaram, J. S., Palanichamy, R. A., & Brohi, S. N. (2017). An Integrated Real-Time Simulated Ethical Hacking Toolkit with Interactive Gamification Capabilities and Cyber Security Educational Platform. *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence*, 199–202. https://doi.org/10.1145/3168390.3168397

Park, C., Kontovas, C., Yang, Z., & Chang, C.-H. (2023). A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management*, *235*, 106480. https://doi.org/10.1016/j.ocecoaman.2023.106480

*The impact of gamification in educational settings on student learning outcomes: A meta-analysis | Educational technology research and development*. (n.d.). Retrieved June 14, 2024, from https://link.springer.com/article/10.1007/s11423-020-09807-z

Ciussi, D. M. (2018). *ECGBL 2018 12th European Conference on Game-Based Learning*. Academic Conferences and publishing limited.

*Cybersecurity awareness and market valuations—ScienceDirect*. (n.d.). Retrieved July 2, 2024, from https://www.sciencedirect.com/science/article/abs/pii/S0278425418302370

Hart, S. (2022). *A pedagogical design model to create serious games for cyber security* [Phd, University of Southampton]. https://eprints.soton.ac.uk/457783/

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*, *95*, 101827. https://doi.org/10.1016/j.cose.2020.101827

Hu, S., Hsu, C., & Zhou, Z. (2022). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, *62*(4), 752–764. https://doi.org/10.1080/08874417.2021.1913671

Kadena, E., & Gupi, M. (2021). HUMAN FACTORS IN CYBERSECURITY: RISKS AND IMPACTS. *Security Science Journal*, *2*(2), Article 2.

Khan, N. F., Ikram, N., Murtaza, H., & Asadi, M. A. (2021). Social media users and cybersecurity awareness: Predicting self-disclosure using a hybrid artificial intelligence approach. *Kybernetes*, *52*(1), 401–421. https://doi.org/10.1108/K-05-2021-0377

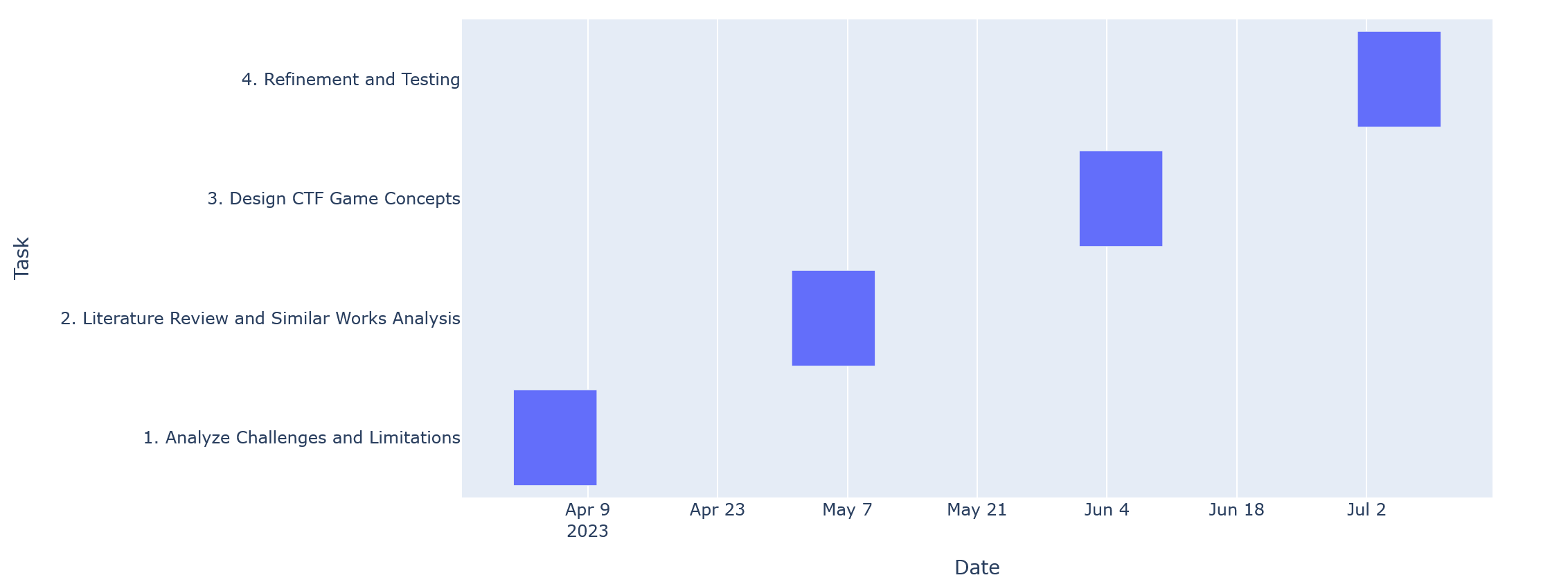
Koohang, A., Anderson, J., Nord, J. H., & Paliszkiewicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, *120*(1), 231–247. https://doi.org/10.1108/IMDS-07-2019-0412

Mathoosoothenen, V. N., Sundaram, J. S., Palanichamy, R. A., & Brohi, S. N. (2017). An Integrated Real-Time Simulated Ethical Hacking Toolkit with Interactive Gamification Capabilities and Cyber Security Educational Platform. *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence*, 199–202. https://doi.org/10.1145/3168390.3168397

Park, C., Kontovas, C., Yang, Z., & Chang, C.-H. (2023). A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management*, *235*, 106480. https://doi.org/10.1016/j.ocecoaman.2023.106480

*The impact of gamification in educational settings on student learning outcomes: A meta-analysis | Educational technology research and development*. (n.d.). Retrieved June 14, 2024, from https://link.springer.com/article/10.1007/s11423-020-09807-z

# GANTT CHART



**BSC. IN COMPUTER NETWORKS AND CYBER SECURITY**

**PROPOSAL MARKING GUIDE**

**CNS Project II**

**Section A – Student’s Details:**

|  |  |
| --- | --- |
| **Student Number** | **Student Name** |
|  |  |
| **Project Title:** |  |

**Section B – For examiner’s use only:**

|  |  |  |
| --- | --- | --- |
| **Area of Assessment** | **Score** | **Total** |
| **Title (2)** |  |  |
| - Is the title informative, concise, focused and appropriate? *(2)* |  |  |
| **Abstract (3)** |  |  |
| - Describes the concept clearly *(3)* |  |  |
| **Introduction (6)** |  |  |
| * Is there a clear identification of a specific problem that relates to a Computer Network and Cyber Security challenge? *(1)* * Are the objectives S.M.A.R.T and incremental? *(2)* * Do the objectives support the achievement of the project’s aim? *(1)* * Has the significance of the project and justification for undertaking the project been clearly explained? *(1)* * Is the scope achievable at the candidate’s level *(1)* |  |  |
| **Literature Review (11)** |  |  |
| * Has the objective-literature mapping (Literature Review sections to address each Specific Objective) been done correctly? *(3)* * Does the literature review analyse what has been done before in relation to the project, what has not been done (the gap), and what the project proposes to do to address the gap? *(3)* * Has adequate and up to date literature been reviewed? *(3)* * Is the conceptual framework supporting the concept discussed? *(2)* |  |  |
| **Design Methodology (6)** |  |  |
| * Has the correct/fitting design methodology been used. *(2)* * Presents practical implementation plan with a list of tools and systems that will be used *(2)* * Are the deliverables discussed and are they practical and achievable? *(2)* |  |  |
| **Overall Assessment (12)** |  |  |
| * Is there a logical mapping from the Title, to the Objectives, to the Literature Review topics, to the Methodology, to the proposed tools to be used, and lastly to the deliverables? *(3)* * Proposal document is neat and well formatted. Table of contents numbered in sequence and corresponds to page Numbers *(3)* * Evidence that figures were drawn by candidate and not copy pasted *(2)* * Has the APA referencing style been correctly applied? *(1)* * Demonstrates that candidate will learn from the project *(3)* |  |  |
| **TOTAL (40)** |  |  |

Page **1** of **2**

**Please provide further feedback for the candidate:**

**Examiner** *(initials)* **Date:**