

**Ain Shams University**  
**Faculty of Computer & Information Sciences**

**Cyber Security Program**

**Cyber Learning Adventure (Junior)**

**May 2022**



**By:**

Omar Ahmed Wafaa Eldeen [Cyber Security]

Abdelrahman Mohamed Kamal [Cyber Security]

Ahmed Essam El-Deen Mohamed Ahmed [Cyber Security]

David Moheb Anwar [Cyber Security]

Omar Magdy Abdelhamed Nassar [Cyber Security]

**Cyber Learning Adventure (Junior)**

**Under Supervision of:**

[Hanan Hindy]

[PhD],

Computer Science Department,

Faculty of Computer and Information Sciences,

Ain Shams University.

**Ain Shams University**  
**Faculty of Computer & Information Sciences**

**Cyber Security Program**

# Acknowledgement

If you want to include thank you notes to any one you should put it here. (The acknowledgement is optional)

# Abstract

The abstract is one page summary of the whole project including: why the project is needed, what are the main features of the project and what are the final results obtained by the developed system.

It’s the most important page in the whole documentation, it should be the last thing you write.

**Table of Contents**

[Acknowledgement i](#_Toc417741593)

[Abstract ii](#_Toc417741594)

[List of Figures iv](#_Toc417741595)

[List of Abbreviations v](#_Toc417741596)

[1- Introduction 1](#_Toc417741597)

[1.1 Motivation 1](#_Toc417741598)

[1.2 Problem Definition 1](#_Toc417741599)

[1.3 Objective 1](#_Toc417741600)

[1.4 Time Plan 1](#_Toc417741601)

[1.5 Document Organization 1](#_Toc417741602)

[2- Background 2](#_Toc417741603)

[3- Analysis and Design 3](#_Toc417741604)

[3.1 System Overview 3](#_Toc417741605)

[3.1.1 System Architecture 3](#_Toc417741606)

[3.1.2 System Users 3](#_Toc417741607)

[3.2 System Analysis & Design 3](#_Toc417741608)

[3.2.1 Use Case Diagram 3](#_Toc417741609)

[3.2.2 Class Diagram 3](#_Toc417741610)

[3.2.3 Sequence Diagram 3](#_Toc417741611)

[3.2.4 Database Diagram 4](#_Toc417741612)

[4- Implementation and Testing 5](#_Toc417741613)

[5- User Manual 6](#_Toc417741614)

[6- Conclusion and Future Work 7](#_Toc417741615)

[6.1 Conclusion 7](#_Toc417741616)

[6.2 Future Work 7](#_Toc417741617)

[References 8](#_Toc417741618)

# List of Figures

[**Figure 1- Neural Network general architecture** 4](#_Toc417423219)

Note: Always number your figures and include a caption under each one like this. Then if you update the list above it’ll be updated automatically.

When adding a figure, right click on the image -> insert caption.

After you finish the document, write click on the table and choose update field, then update entire table.



**Figure 1- Neural Network general architecture**

Add list of Tables if you have tables in your text in the same manner

# List of Abbreviations

|  |  |  |
| --- | --- | --- |
| Abbreviation | What the abbreviation stands for |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Note: Any abbreviations used throughout the document should be included here. The list should be sorted **alphabetically**.

# Introduction

## 1.1 Motivation

To help children in gaining the necessary awareness to protect themselves against the threats they can face while using the internet because the only available awareness-providing tools are aimed at adults and are far too advanced for children.

## 1.2 Problem Definition

Since the Covid-19 pandemic, kids nowadays spend a lot of time in front of screens on daily basis. And with lack of awareness, children are exposed to a new set of threats as their use of web-based tools, downloading new applications, and reliance on email grows.

## 1.3 Objective

* Offering a gamified and enjoyable way for kids to learn about cyber security threats and attacks.
* Providing a simple, yet efficient ways to report security attacks.
* Implementing practical hands-on experience.

## 1.4 Time Plan

Graphical user interface

Description automatically generated

## 1.5 Document Organization

Chapter 2 explains different topics regarding the Background of the project such as The field of the project, a survey of the work done in this field, The scientific background related to the project, similar systems to the game and technologies used. Chapter 4 is about the implementation and testing, this part describes all the functions used in the system, all the techniques and algorithms used, Description of any new technologies used in implementation & Testing procedures and levels used. Chapter 5 includes the user manual. In Chapter 6, the project is summarized with the results obtained and the future work is stated.

# Background

* The field of Cyber Learning Adventure (Junior) is mainly Cyber Security besides multimedia.
* Scientific background related to the project:

-Gamification

The idea behind gamification is enriching products, services, and information systems with game-design elements in order to positively influence motivation, productivity. Gamification is a persuasive technology that attempts to influence user behavior by activating individual motives via game-design elements. The idea of gamification is spawning an intense public debate as well as numerous applications ranging across productivity, finance, health, education, sustainability, as well as news and entertainment media. Several vendors now offer “gamification” as a software service layer of reward and reputation systems with points, badges, levels and leader boards. More specific notion is that since video games are designed with the primary purpose of entertainment, and since they can demonstrably motivate users to engage with them with unparalleled intensity and duration, game elements should be able to make other, non-game products and services more enjoyable and engaging as well.

Games with a purpose reflect an approach in which problems that cannot satisfactorily be solved with information systems are transformed, so that human individuals can solve them in a game-like fashion. The potential of gamification is based on comprehensive motivational support and on invoking flow experiences. IT-based gamified enhancing services are able to arouse the intrinsic motivation of users regarding a core offer:

• Increase in user satisfaction.

• Conveyance of optimism.

• Facilitation of social interaction.

• Provision of meaning.

-Capture the flag challenges and how they are created

Capture the Flag challenges are a popular form of cybersecurity education, where students solve hands-on tasks in an informal, game-like setting. The term “Capture the Flag” originally refers to an outdoor game for two teams. Each team must simultaneously defend a (physical) flag in their base and steal the other team’s flag. CTF tasks, called challenges, feature diverse assignments from exploiting websites, through cracking passwords, to breaching unsecured networks. A successful solution of a challenge yields a text string called a flag that is submitted online to prove reaching the solution. Three types of CTF games are generally distinguished: quiz based, in which participants score points by answering questions; scavenger-hunt, or flag-based, in which participants locate and exploit vulnerabilities in systems security in order to gain access to files which contain “flags” in the form of random strings, and king-of-the-hill, or castle-based, in which participants score points by defending a server against attackers. Capture the Flag (CTF) competitions are very popular for testing skills and presenting challenges for practice on various security topics such as cryptography, steganography, web or binary exploitation and reverse engineering among others. Capture the Flag challenges should also include non-technical aspects to address the current advanced cyber threats and attract audience to cybersecurity. CTF tasks showed the prominence of technical knowledge about cryptography and network security, but human aspects, such as social engineering and cybersecurity awareness are neglected, which we will focus on. By introducing gamification components, a shared scoring system to encourage some friendly competition, and the ability to buy hints using points that were scored by solving previous challenges, we anticipate that students will enjoy participation in the CTF. By active participation, students will spend more time learning and develop stronger outcomes. Overwhelmingly, participants were able to define and explain the consequences of password re-use, phishing and weak configurations. Significant increases in outcomes will be observed in participants’ ability to describe the risks of using weak passwords. Self-confidence of students will improve by participating in (CTFs). Participating in the CTF reinforces theoretical concepts.

-Cyber threats on kids

The internet can be a dangerous neighborhood for everyone, but children and teens are especially vulnerable. From cyber predators to social media posts that can come back to haunt them later in life, [online hazards](https://usa.kaspersky.com/resource-center/threats/web) can have severe, costly, even tragic, consequences. Children may unwittingly expose their families to [internet threats](https://usa.kaspersky.com/resource-center/threats/top-7-cyberthreats), for example, by accidentally downloading [malware](https://usa.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs) that could give [cyber criminals](https://usa.kaspersky.com/resource-center/threats/cybercrime) access to their parents' bank account or other sensitive information. Protecting children on the internet is a matter of awareness—knowing what dangers lurk and how to safeguard against them.

-Cyber threat modelling

Almost all software systems today deal with a range of threats, and new ones are continually being added as technology evolves. These threats can emerge from both inside and outside of organizations, and their impact can be severe. Systems could be rendered inoperable, or sensitive information could be disclosed, eroding user trust in the system provider. [1] Therefore, any organization shall be ready for any consequences and know how to act upon that.

As the world has gotten more digital, cyber assaults have become more regular and frequent; as a result, threat modelling is no longer an optional activity. Threat modelling can assist you in making your product safer and trustworthy. As there are many threat models out there, some of which are typically used alone, some are usually used in conjunction with others, and some are examples of how different methods can be combined, No one threat modelling method is recommended over another; the decision of which method(s) to use should be based on the needs of the project and its specific concerns like are there any specific areas you want to target (risk, security, privacy), or how long you have to perform threat modelling.

-How kids use the internet

According to best estimates one in three children around the world now uses the internet.

First things first, why is the internet rapidly used by children? Internet is fast becoming trusted by both children and adults as reliable and accurate sources of information. Through the internet children now can have access to an almost endless supply of information and opportunity for interaction. However, there can be real risks and dangers for an unsupervised child.

Since the start of the pandemic, governments worldwide have implemented measures to contain the spread of covid-19, one of which is school closures all over the world. As a result, e-learning has become a viable solution. Internet usage can be a medium of learning online, the information related to the task as well as the latest information can impact the cognitive development.

In Indonesia, until the 1990s, after school, children used to go out with their friends to play together and interact among each other. But during these times, this condition has become very rare. This is due to the child “net generation” tends to use the internet as fun activity for them. With using the internet, their needs are met such as obtaining entertainment.

Social media is another aspect that makes children use internet. The internet facilitates communication with geographically distant family and friends as well as making it easier to communicate frequently with those nearby. There is another of advantage of social media which is making new friends through games and groups made on social media.

* Work done in the field

-H. M. Jawad and S. Tout, "IEEE Xplore," in Introducing a Mobile App to Increase Cybersecurity Awareness in MENA, Dubai, 2021.

-I. M.Venter, R. J.Blignaut, K. Renaud and M. A. Venter, "Cyber security education is as essential as “the three R's”," Heliyon, vol. 5, no. 12, 2019.

-F. Quayyum, D. S.Cruzes and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," International Journal of Child-Computer Interaction, vol. 30, 2021.

-H. M. Jawad and S. Tout, "IEEE Xplore," in Introducing a Mobile App to Increase Cybersecurity Awareness in MENA, Dubai, 2021.

-"Hacking Training for The Best", Hack The Box, 2021. [Online]. Available: https://www.hackthebox.com/.

-"OWASP Foundation | Open Source Foundation for Application Security", Owasp.org, 2021.

-"Cybersecurity in Education: What Teachers, Parents and Students Should Know | Berkeley Boot Camps", Berkeley Boot Camps, 2021. [Online].

-"Cybertalentskids » CyberTalents", CybertalentKids, 2021.

* Similar Systems:

-CTFs

CTF (Capture The Flag) is a kind of information security competition that challenges contestants to solve a variety of tasks ranging from a scavenger hunt on Wikipedia to basic programming exercises, to hacking your way into a server to steal data. In these challenges, the contestant is usually asked to find a specific piece of text that may be hidden on the server or behind a webpage. This goal is called the flag.

-Cyber Talent kids

CyberTalents Kids is a gamified cybersecurity training platform focusing on kids from 11 to 16 years old across the globe where they can learn, practice, compete, and get ranked. The main goal of CyberTalents Kids is Our mission is to raise cybersecurity awareness to help build the next generation who will lead and shape the future of cybersecurity.

-Cybersmart challenge

Teacher-led activities using animated videos to introduce primary school students to key online safety issues including cyberbullying, protecting personal information and sharing images. The outcome is that the Students will be better equipped to understand and manage key online safety issues, including inappropriate or unwanted contact, cyberbullying and the risks of sharing images online.

-Introducing a Mobile App to Increase Cybersecurity Awareness in Mena Region

This paper introduces a new mobile app in the Arabic language to educate Arab-speaking people in the Middle East and North Africa (MENA) about cybersecurity and to increase their awareness of information assurance and cybercrimes. The app was developed for Android and iOS devices, and it includes multiple-choice information assurance questions, terms, and articles. Examples of the term definitions are Two-Factor Authentication, Ethical Hacking, and Honeypot.

* Technologies used:
* Game Engine

-Unity

* Programming Language

-C#

* Code IDE

-Visual Studio

* Graphics Tool

-Gimp

-Photoshop

# Analysis and Design

## 3.1 System Overview

### 3.1.1 System Architecture

Include a figure of the system architecture and a description of all modules.

You may add Functional and non-functional requirements section –If needed–

### 3.1.2 System Users

1. *Intended Users:*

To whom the system is built, and how each group of users will use the system.

1. *User Characteristics*

What kind of experience or skills are required from the users to be able to operate the project effectively.

## 3.2 System Analysis & Design

### 3.2.1 Use Case Diagram

The use case diagram + fully dressed use cases describing each function of the project if applicable.

### 3.2.2 Class Diagram

The diagram + description of all the main classes if applicable.

### 3.2.3 Sequence Diagram

if applicable

### 3.2.4 Database Diagram

If you are implementing a database include the database schema plus a description of the tables.

# Implementation and Testing

This chapter should include:

* A detailed description of all the functions in the system.

-Player Movement

Where the player can move freely in two directions (left and right) and jump.

-Dialogue System

It is a is a gameplay mechanic where the player interacts with non-player character and the player is given a choice of what to say and makes subsequent choices until the conversation ends.

* A detailed description of all the techniques and algorithms implemented.
* Description of any new technologies used in implementation.
* UI Design and Wireframes
* Testing procedures and levels used

# User Manual

This chapter should describe in details how to operate the project along with screen shots of the project representing all steps.

This chapter should also include an "Installation Guide" that would describe how to install the program, and all required third party tools that needs to be available for the project to run. The installation guide will also be included as a readme file in the CDs delivered at the end of the year.

# Conclusion and Future Work

## 6.1 Conclusion

A complete summary of the whole project along with the results obtained.

The game is divided in two versions, the first version contains different password levels from easy to hard and one sublevel for phishing. It also contains the main menu and about section which shows information about the game. Settings scenes and screen were also created, and it contains reset option to reset the progress of the player. The second version contains the gamified design and UIs of the game.

## 6.2 Future Work

* Implement more levels
* Improve the gamification to make it more enjoyable and attractive for the kids
* Transfer phishing levels from game1 to game2
* Create Leadership for Motivation
* Implement reward system

**References**

* [1]"Screen time 'may harm toddlers'", BBC News, 2019. [Online]. Available: https://www.bbc.com/news/health-47026834. [Accessed: 06- Dec- 2021].
* [2]"Cybersecurity in Education: What Teachers, Parents and Students Should Know | Berkeley Boot Camps", Berkeley Boot Camps, 2021. [Online]. Available: https://bootcamp.berkeley.edu/blog/cybersecurity-in-education-what-teachers-parents-and-students-should-know/. [Accessed: 06- Dec- 2021].
* [3]"Cybertalentskids » CyberTalents", CybertalentKids, 2021. [Online]. Available: https://cybertalentskids.com/. [Accessed: 06- Dec- 2021].
* [4]2021. [Online]. Available: https://www.esafety.gov.au/educators/classroom-resources/cybersmart-challenge. [Accessed: 06- Dec- 2021].
* [5]H. M. Jawad and S. Tout, "IEEE Xplore," in Introducing a Mobile App to Increase Cybersecurity Awareness in MENA, Dubai, 2021. [Accessed: 06- Dec- 2021].
* [6]"Hacking Training For The Best", Hack The Box, 2021. [Online]. Available: https://www.hackthebox.com/. [Accessed: 06- Dec- 2021].
* [7]"OWASP Foundation | Open Source Foundation for Application Security", Owasp.org, 2021. [Online]. Available: https://owasp.org/. [Accessed: 06- Dec- 2021].
* [8]M. Robb, "Common Sense Media," Common Sense Media, 29 October 2019. [Online]. Available: https://www.commonsensemedia.org/blog/tweens-teens-and-phones-what-our-2019-research-reveals#:~:text=A%20majority%20(53%25)%20of,2019%20from%2011%25%20in%202015.. [Accessed 08 November 2021].
* [9]Kaspersky, "Kaspersky," Kaspersky, [Online]. Available: https://usa.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online. [Accessed 08 November 2021].
* [10]DQ Institute, "DQ Institute," DQ Institute, [Online]. Available: https://www.dqinstitute.org/child-online-safety-index/. [Accessed 08 November 2021].
* [11]C. Li, "Weforum," World Economic Forum, 29 April 2020. [Online]. Available: https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/. [Accessed 08 November 2021].
* [12]J. Johnson, "Statista," 06 May 2021. [Online]. Available: https://www.statista.com/statistics/1189204/us-teens-children-screen-time-daily-coronavirus-before-during/. [Accessed 08 November 2021].
* [13]Unicef, "Unicef," Unicef, 04 February 2021. [Online]. Available: https://www.unicef.org/coronavirus/keep-your-child-safe-online-at-home-covid-19. [Accessed 10 November 2021].
* [14]H. M. Jawad and S. Tout, "IEEE Xplore," in Introducing a Mobile App to Increase Cybersecurity Awareness in MENA, Dubai, 2021.
* [15]I. M.Venter, R. J.Blignaut, K. Renaud and M. A. Venter, "Cyber security education is as essential as “the three R's”," Heliyon, vol. 5, no. 12, 2019.
* [16]F. Quayyum, D. S.Cruzes and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," International Journal of Child-Computer Interaction, vol. 30, 2021.