**An approach for malware analysis using hashing**

Submitted in partial fulfillment of the requirement of the degree

**BACHELOR OF ENGINEERING IN COMPUTER ENGINEERING**

By

**Anuj R Tiwari 19CE1088**

**Prathamesh S Vanjape 19CE1010**

**Rohan B Tirmakhe 19CE1036**

Supervisor

**Mrs. Tabassum Maktum**



**Department of Computer Engineering Dr. D. Y. Patil Group’s Ramrao Adik Institute of Technology**

**Dr. D. Y. Patil Vidyanagar, Sector 7, Nerul, Navi Mumbai 400706. University of Mumbai**

**(Ay 2020-21)**

**CERTIFICATE**

This is to certify that the Mini Project entitled **“An approach for malware analysis using hashing”** is a bonafide work of **Prathamesh S Vanjape (10CE1010), Rohan B Tirmakhe (19CE1036), Anuj R Tiwari (19CE1088)** submitted to the University of Mumbai in partial fulfillment of the requirement for the award of the degree of

**“Bachelor of Engineering”** in **“Computer Engineering”.**

( **Mrs. Tabassum Maktum** )

Supervisor

**( Dr. Leena Ragha ) ( Dr. Mukesh D. Patil )**

Head of Department Principal

**Mini Project Approval**

This Mini Project entitled “**An approach for malware analysis using hashing”** by **Prathamesh S Vanjape (19CE1010), Rohan B Tirmakhe (10CE1036)** and **Anuj R Tiwari (19CE1088)** is approved for the degree of **Bachelor of Engineering** in **Computer Engineering.**

## Examiners

**1…………………………………………**

(Internal Examiner Name & Sign)

**2…………………………………………**

(External Examiner name & Sign)

Date: Place:

# Abstract

Malware is a short form of MALICIOUS SOFTWARE, which is a collective phrase for all software developed for disrupting, damaging or gaining access to data and systems in an unauthorized manner. Malware has remained a consistent threat since its emergence, growing into a plethora of types and in large numbers. Malware Authors have managed to increase their malware’s sophistication to avoid detection against anti-malware technics by implementing new features and specific modifications, such as encryption, polymorphism and metamorphism to maximize their resilience. However, anti-virus vendors and analysts managed to adapt their identification techniques by relying on automated analysis methods, and tools in order to distinguish malicious from benign code, such as the traditional static analysis using Cryptographic hashes with the MD5 and SHA256 being the most commonly used in Malware Research in 2013.

## Acknowledgement

We take this privilege to express our sincere thanks to Dr. Mukesh D. Patil, Principal, RAIT for providing the much necessary facilities. We are also thankful to Dr. Leena Ragha, Head of Department of Computer Engineering, Project Co-ordinator Dr. Vanita Mane, Department of Computer Engineering, RAIT and Project Guide Mrs. Tabassum Maktum, Department of Computer Engineering, RAIT for their generous support.

We take this opportunity to express our profound gratitude and deep regards to our guide Mrs. Tabassum Maktum for her exemplary guidance, monitoring, and constant encouragement throughout the completion of this report. We are truly grateful for her efforts to improve my understanding of various concepts and technical skills required in our project. The blessing, help, and guidance given by her from time to time shall carry us a long way in the journey of life on which we are about to embark.

Last but not least we would also like to thank all those who have directly or indirectly helped us in the completion of this thesis.

# List of Figures

3.1 Architecture Framework 5

3.2 Use Case Diagram 7

3.3 Activity Diagram 8

3.4 Main Page 9

3.5 Custom Words Page 10

3.6 Categories Page 10

3.7 Game Page 11

3.8 Single Player Score Board 11

3.9 Multiplayer Score Board 12

## Contents

**Abstract i**

**Acknowledgments ii**

**List of Figures iii**

1. **Introduction 1**

Introduction 1

Motivation 1

Problem Statement & Objectives 2

Organization of the Report 2

1. **Literature Survey 3**

Survey of Existing System3

Limitation of existing system or research app3

Mini Project Contribution4

1. **Proposed System 5**

Architecture/Framework5

Process of Malware Analysis 6

Details of Project (Hardware & Software)8

Experiment and Result9

1. **Conclusion and Future Work 13**

### 1. Introduction

Malware is a short form of MALICIOUS SOFTWARE, which is a collective phrase for all software developed for disrupting, damaging or gaining access to data and systems in an unauthorized manner. Malware has remained a consistent threat since its emergence, growing into a plethora of types and in large numbers. Malware Authors have managed to increase their malware’s sophistication to avoid detection against anti-malware technics by implementing new features and specific modifications, such as encryption, polymorphism and metamorphism to maximize their resilience. However, anti-virus vendors and analysts managed to adapt their identification techniques by relying on automated analysis methods, and tools in order to distinguish malicious from benign code, such as the traditional static analysis using Cryptographic hashes with the MD5 and SHA256 being the most commonly used in Malware Research in 2013.

The project aims to design a game “An approach for malware analysis using hashing” in which a. malware authors have managed to increase their malware’s sophistication to avoid detection against anti-malware technics by implementing new features and specific modifications, such as encryption, polymorphism and metamorphism to maximize their resilience .

**1.1. Motivation:**

Games are played for enjoyment, sometimes for achievement or reward as well. A Video Game is an electronic game that involves interaction with a user interface. Currently, there is a large demand for games in the market and is exponentially increasing. We aimed to develop one such game with a simple yet interesting user interface to provide entertainment. We also had an aim to give it a slight touch for Education too. In this pandemic, education is shifting from offline to online mode. In this situation, a better way of learning for kids will be through games.

**1.2. Problem Statement and Objective:**

The project aims to create a Malware Analysis Tool. There are a number of different ways of categorizing malware and the most common types of malwares are:

1)Worms

2)Virus

3)Trojan

The basic idea of the project is to use the hashing or other encryption algorithm to find an efficient way for malware analysis

**Objective:**

The main motive of this topic is to develop a user friendly and interactive game jumble words. Other aims while developing the games were

* To design jumble word with different modes
* To making it interesting with different categories  To allow users to add custom words

**1.3. Organization of Report:**

This report gives a brief summary of the project which includes details about every component of the project. Chapter 1 is an introduction to the project and tells motivation for developing this project and objectives about it and also gives an overview of the project. Chapter 2 is a literature survey we made while analyzing all the requirements of the project. In Chapter 3 we have mentioned architecture design/framework, implementation details, the technology used to develop the system, and results. In Chapter 4 conclusion and future work are described. Chapter 5 consists the references that have been used while developing this project.

### 2. Literature Survey

**2.1. Survey of Existing System:**

Similar games have been found on Play-store and other sites. For developing our game the most important thing was to survey the existing games present at present in the market and noting down their main features and the features which are lacking in them. While surveying we came across many such games. On viewing the review of the games we got details about the features which users liked the most as well as the features which users didn’t want in the game.

Some Examples of our surveyed games are Listed Below:-

1. **JUMBLE Word Puzzle:** It is a classic Jumble word game which provides users option to guess the correct words along with the hints and timer. It also provides options for Background. However the game doesn’t has a Multiplayer mode as well

as it contains adware. **[1]**

1. **Plato:** Games & Group Chats: It is a multiplayer games covering the limitation of the above games but lacking some of the most important features such as Timer.

As it has many games the GUI of the game doesn’t look clean and user friendly**.[2]**

**2.2. Limitation of Existing Games or Apps:**

The Existing System Were lacking many points:

* **ADWARE:** One of the most irritating one’s while enjoying a game. Earning from add is acceptable but filling the whole screen with add ware causes a lack of interest for users towards the game.
* **COMPLEX GUI:** Trying to fit everything in a page causes clustering in a page. It doesn’t feel like a user friendly system.
* **NO CUSTOMIZATION:** Especially in a game like Jumble Words playing with the same words makes it boring. So accepting the words from the user to Challenge each other gives such type of game an upper edge.
* **TIMER:** One of the most important feature of jumble word game is a Timer. If there is no timer in the game user can take decades to guess a words. Providing a customizable timer can be one of the best features for while setting the difficulty level of the game by the user.

On surveying, we came across many limitations as well as many interesting features in the games. But there was no such game having the combination of the features mentioned above which are the must include the feature for the game of this type. For example, the Plato game had a very interactive GUI with a chat system between the players but instead of having such a great feature it was missing the timer and customization part.

Whereas the jumble puzzle game had the timer but it didn’t have an option to add custom words, as well as the whole game page, was getting filled up with ads. So we came across the solution of making the limitations mentioned above, the main features of our game.

**2.3. Mini project Contribution:**

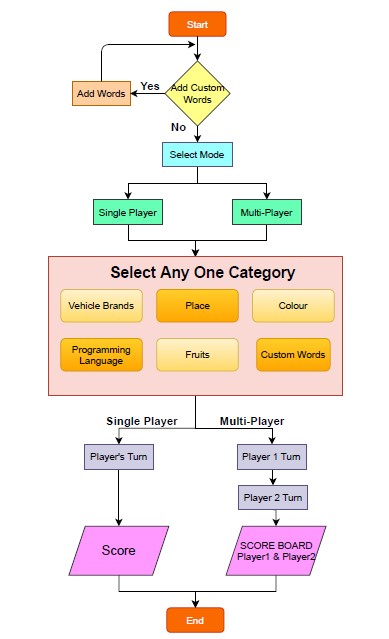
Jumble Word is an interactive puzzle game. It is a brainstorming game that will let users learn new words while playing it. Increasing vocabulary and general knowledge are other great advantages for children while playing the game. The game provides an excellent platform in education as well. Another important factor is that this game encourages problem-solving abilities in kids.

### 3. Proposed System

**3.1. Architecture/Framework:**

The proposed model is shown below. The user gets an option to select whether he/she wants to custom words in the game which will be updated in the custom file in the local system after which he/she can either select the mode or can add more custom words. While adding the custom words the words stored in the file during the previous time the game was placed will get replaced with the new words. After that, the user has to select whether he/ she wants to play the game in single or multiplayer mode following which he has to choose the category from the five pre-entered categories and one custom category.

After which game page will appear following the scoreboard.



#### Figure 3.1 Architecture Framework

**3.2. Algorithm and Process Design:**

**Algorithm:**

Algorithm means a process or a set of rules that needs to be followed. Therefore algorithm refers to a set of rules/instructions that step by step define how a work is to be executed upon in order to get the expected result. Algorithms are language independent that is they are just plain instructions that can be implemented in any language, and yet the output will be the same, as expected. The algorithm that is the basic set of instructions that users can opt for fir desired output is shown below.

Step 1: Start

Step 2: Select mode

If mode == custom

Then Add new words

Else

Go to step 3

Step 3: Select single player mode or multiplayer mode or add more words

If mode == add more words

Then Add more words

Else

Go to step 4

Step 4: Select any one of the predefined categories

Step 5: Guess the correct word within the given timer and chances available

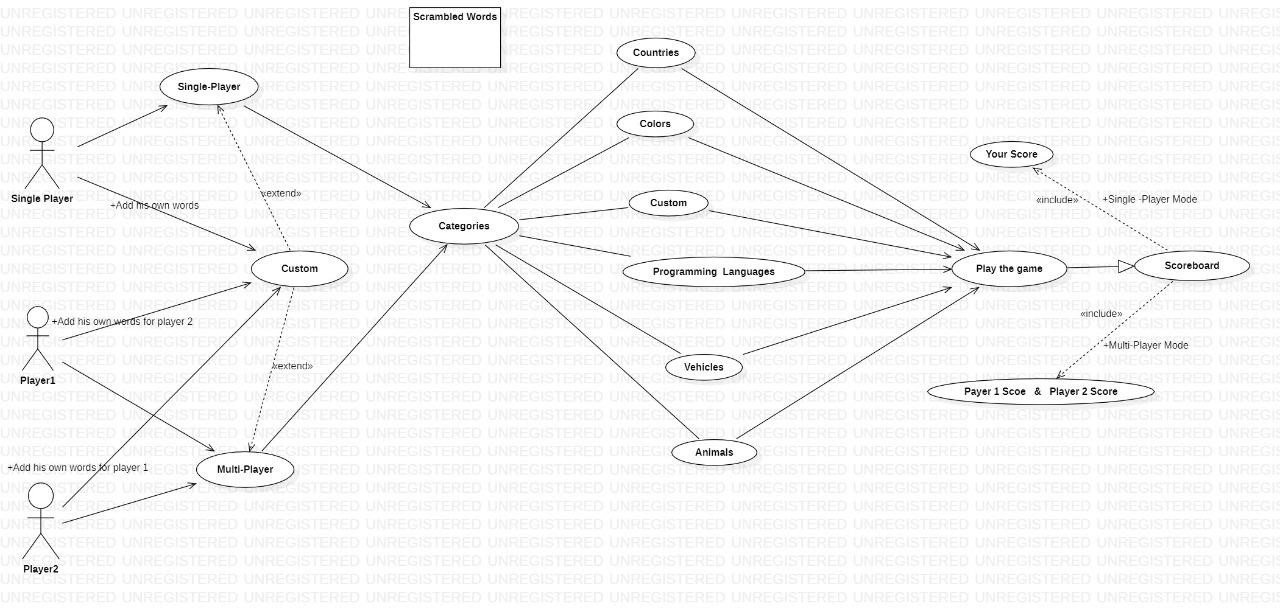
Step 6: Display of Scoreboard

Step 6: Stop

**Process Design:**

 **Use Case Diagram**

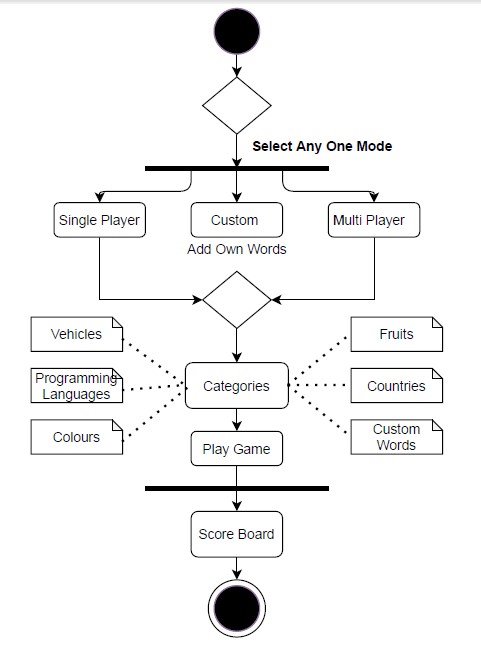
A use case diagram is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved. A single use case diagram captures a particular functionality of a system. Here use case diagram of “Jumble Words” is given.



#### Figure 3.2 Use Case Diagram

 **Activity Diagram:**

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. It is a behavioral diagram. The activity can be described as an operation of the system. The control flow is drawn from one operation to another.



#### Figure 3.3 Activity Diagram

**3.3. Details of Hardware & Software:**

The Language we have used in this project is PYTHON. The libraries used from Python language are

* **Pygame:** Pygame is a cross-platform set of Python modules which is used to create video games. It is one of the most advanced video game library. It is widely used by the developers. However we used this library to provide Music to our game. **[3]**
* **Tkinter:** Tkinter is the standard GUI library for Python. Python when combined with Tkinter provides a fast and easy way to create GUI applications. Our main project part is programmed using Tkinter library. We chose this library as it gave us an option to create multiple frames which was a key need in our project. **[4]**

**3.4. Experiment and Result:**

The most important features in the game were to create a multiplayer mode, the custom option and timer. We have also added a background music in the game to make it more interesting.

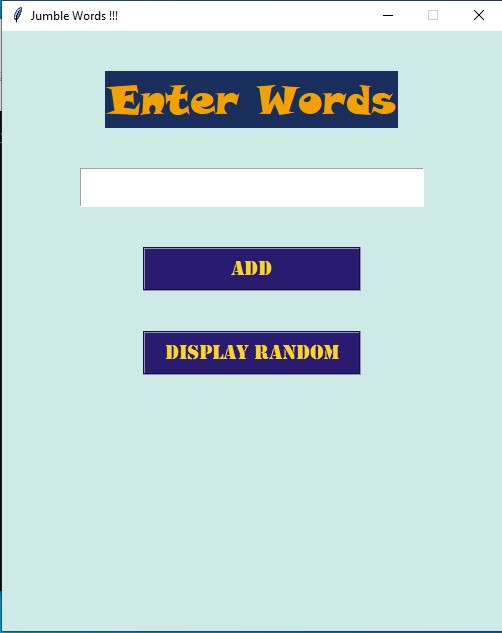
Below are the final pages/frames of our game:

* **Main Page:** It is the main page of our game it consists of three buttons which are single player, multiplayer and add custom words page.



#### Figure 3.4 Main Page

**Custom words page:** Custom words can be added here if users want to challenge each other. From here they can either add more words in the game or they can view the words they have entered in jumble form from where they can play the game.



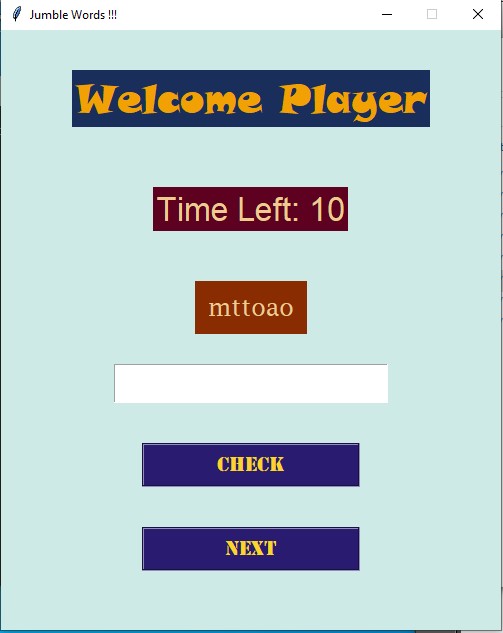
#### Figure 3.5 Custom Words Page

 **Categories page:** After selecting the mode that is either single player or multiplayer mode they can choose their category of words they want to play with including the custom words category.



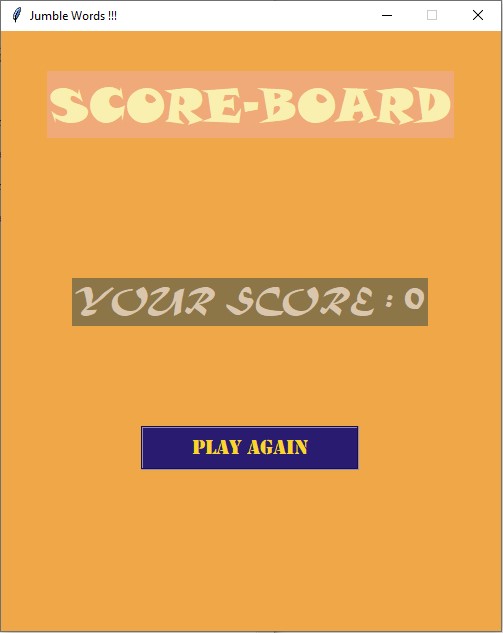
#### Figure 3.6 Categories Page

**Game page:** It is the main page of our game having the jumbled word, time left in game and label of which player’s turn is there. User can either check whether guessed word is correct or not or he/she can skip the word.



#### Figure 3.7 Game Page

 **Scoreboard Page:** Here the score of game will be displayed for single player mode.



#### Figure 3.8 Single Player Score Board

**Scoreboard Page**: Here the score of game will be displayed for multiplayer mode.



**Figure 3.9 Multiplayer Score Board**

### 4. Conclusion and Future Work

Gaming has gained a lot of attention in recent years. In this report, survey is described briefly on games based on similar concept. In the beginning of report main objective of this topic is described. Currently the jumbled word game is designed with different modes and different categories for words. The custom mode feature allows player add own word and challenge opponent and makes the game more interesting. The background music is also added in the game.

**Future Scope**

* Add customizable timer to a players turn so that they can answer as many questions as possible depending on their capability.
* Create an online multiplayer mode for players at two different systems with a chat system for communication between them.

### References

1. Jumble word Puzzle Game: [**https://play.google.com/store/apps/details?id=com.panagola.game.jumblefree&hl=en\_I N&gl=US**](https://docs.python.org/3/library/tkinter.html)
2. Plato Game: [**https://play.google.com/store/apps/details?id=com.plato.android&hl=en\_IN&gl=US**](https://docs.python.org/3/library/tkinter.html)
3. Pygame Library: [**https://www.pygame.org/docs/**](https://www.pygame.org/docs/)
4. Tkinter Library: [**https://docs.python.org/3/library/tkinter.html**](https://docs.python.org/3/library/tkinter.html)