TAISER 2

Training for AI-based cyber Security Engineering Research 2

Sajal Shrestha
Dept. of Computer Science & Engineering
University of Nevada, Reno
Reno, United State
sajal@nevada.unr.edu

Dr. Sushil Louis
Dept. of Computer Science & Engineering
University of Nevada, Reno
Reno, United State
sushil.louis@gmail.com

***Abstract*—TAISER (T2) provides a platform to collect data for the human's behavioral study when working with a Human and an AI as a teammate. This study is a collaboration between the Department of Computer Science & Engineering and the Department of Psychology. T2 collects different latencies, users' choices, and many other data of a user for the study. This project will advance educational knowledge in the fields of AI, cybersecurity, and behavioral science through three objectives, resulting in 1) AI-Enabled Defense Simulation Suite (AI-EDSimS), enabling hands-on learning for students and cybersecurity professionals, 2) a new course on AI and Cybersecurity transforming undergraduate education by integrating the two subjects with a focus on AI-human teaming for proactive cybersecurity practice, and 3) new knowledge in AI-Cybersecurity education as it relates to AI-human teaming, leading to improved understanding of the role of trust and cooperation in AI-human teams. The NSF IUSE: EHR Program supports research and development projects to improve the effectiveness of STEM education for all students. Through the Engaged Student Learning track, the program supports the creation, exploration, and implementation of promising practices and tools.**

***Index Terms*—Human behavior, AI, AI-Human teams, Software engineering, Software requirement**

I. Introduction

The first wave of Artificial intelligence (AI) began in the '80s. It originated from Japan's national initiative of the 5th Generation Computer System, which aimed to produce concurrent logical programming for knowledge processing. Since then the raise of AI has been rapidly growing. AI has been assisting humans for a very long time now. They are rapidly improving in many "human" tasks, ranging from AI in disease diagnosis, AI in language learning, and AI in customer service. AI works to replace human tasks, it can also work against us as well as work with us as teammates.

Here, We want to focus more on AI as a teammate. There has been lots of research and studies about AI and humans working together. Research into human-AI teams is a nascent field and rapidly evolving. AI and people are typically doing some limited work together at a low level, such as a person calling on Alexa or Siri for help. But, what if there is a situation where a human has to decide whether they would want to work with AI or a Human? And what if both AI and Human is your teammate, who do you listen to the most?

Identify applicable funding agency here. If none, delete this.

T2 is a web-based software simulation that collects user data for Human behavior when humans and AI are teammates. It is the second version of TAISER, where T2 solely focuses on studying user behavior working with an AI and a human. T2 stores the different latencies and decisions of the user in a time-ticking situation where the user has to save the networking of the building by filtering malicious packets sent from the backchats. With help of an admin dashboard, we can update the parameter of different behaviors of the game, such as changing the difficulty level, the total number of rounds(waves), etc.

II. Software Development

A. Requirements

T2 is a cyber security-themed game or a simulation where the user will have to filter the malicious packets sent by the black hats by manually setting the rules or by accepting advice from an AI or a Human. Here, a user has to finish the task in time ticking situation in order to save the building's network with the help of an AI and a human. This system reads and writes the data in a file system which is saved as a CSV file on the server. This system contains two game modes; Practice mode: where the user can practice the game as per the instruction, and Session Mode: where the main game mode where the data are collected for the study.

A limited group of students will be a subject for this study, where they won't be given full information about the system but only how to play the game. This simulation might be familiar to those with a Computer Science background as it is Cyber security themed but this system is designed for all kinds of students which is easy to learn after practicing in the practice mode.

A user or a subject will be given a unique alias for every game mode where they first practice it in the Practice mode and later in Session mode. A user will need a headphone to listen to the sound effects of the simulation which will have different psychological effects when they set the correct or incorrect rules and accept advice from an AI or Human. The T2 server can handle as many as a hundred requests per second. It writes the entire data in a single write request to a file when the final round(wave) of the simulation is over.

B. Use Cases

There are two kinds of users: Admin and Subject. Admin can both play the game and also access the admin dashboard to update the parameters of the simulation by including 'admin' in the alias name. While other users, the subjects will not be informed about the admin dashboard. They are simply asked to play in different game modes. A secret key '5' can be pressed to write the default parameters of the simulation.

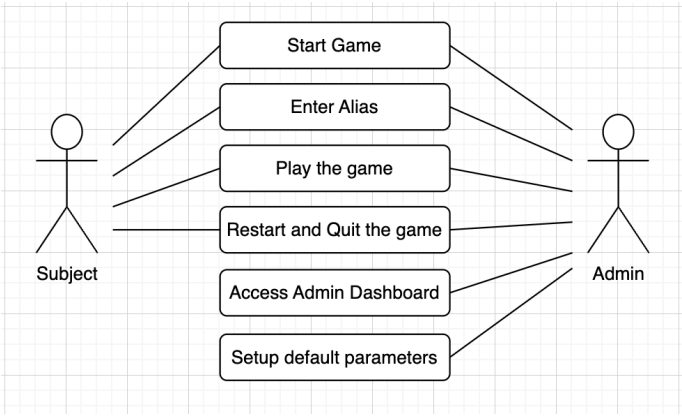

Fig. 1. Users in T2.

A subject is given a unique alias name by the instructor to enter. A subject is expected to read all the 'Mission Objective' panels before clicking the 'Understood' button. After that, a subject should first practice the game as per the instruction for a few waves by clicking on a practice game mode. Then, they shall proceed to Session mode to play the main game.

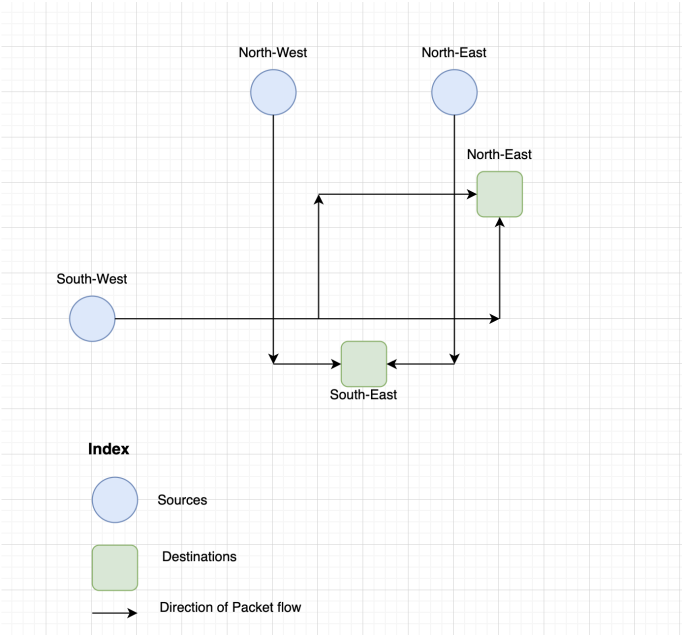

Fig. 2. Sources and Destinations of T2.

There are 3 shapes(Sphere, Cube, Cylinder) and colors(Green, Blue, Pink) packets starts to float from 3 sources(North-West, North-East, and South-West) to 2 destinations(North-East and South-West). This simulation will have one or more rounds which are called waves in this simulation. A source is hidden while the destinations are the building which can be figured by buildings covered by a red wall when the malicious packets hit the buildings. A panel will appear when the user clicks the destination buildings. They have to select whether they want advice from the Human or an AI. After that, They should hover around the packet on the top of the panel and select the red one which is indicated as the malicious bad. Then, the subject filtered the packet by setting the firewall either by manually setting the rules on their own from the left-hand side of the panel, or they can accept advice from the human or ai from the right-hand side. The advice may or may need to be corrected. If the advice is correct the firewall is set and the subject gets points and the red wall of the building decreases. While if the advice, is incorrect they may lose some points or not.

C. Design Architecture

T2 is built using the popular, powerful, and versatile Unity game engine which utilizes C# as the programming language that powers its Scripting API which allows implementing game logic, triggering events, applying physics, responding to user input, checking for collisions and so much more. Unity is a great tool for prototyping everything from games and simulations to interactive visualizations. A singleton design pattern is implemented in C# underneath the Unity game engine. In this pattern, a class has only one instance in the program that provides a global point of access to it.

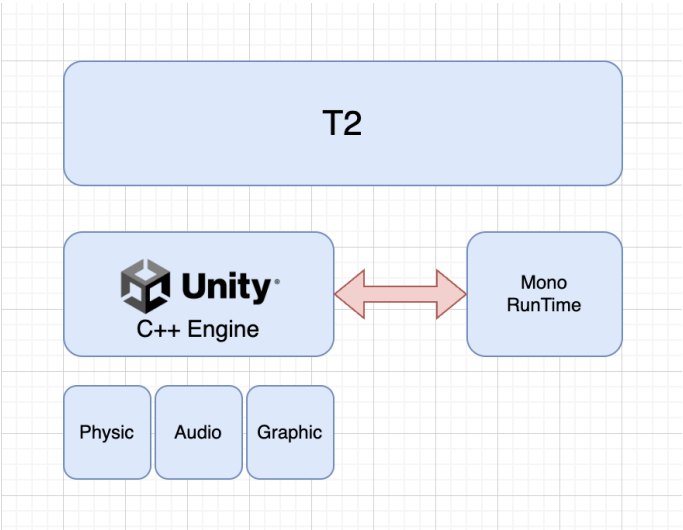

Fig. 3. Unity design architecture.

Unity has its own convention to set up the project structure. There are a set of elements that are used in the Unity game engine; Assets: Assets are basically the project item(s) that can be brought into play in the game or project. The Project – Project in Unity is a folder that contains the entire game project, along with which it contains the assets associated with

the project. GameObject – In simple terms, GameObject is nothing but each and every project that exists within the game or project. Components – Components are the fundamental blocks i.e. the nuts and bolts of objects and their activities in the game. Scenes – A Scene can be defined as the base. where you can position your GameObjects to create a level of your game or project. Prefab – Prefabs are reusable or recyclable components of the game that are present in the Project View window.

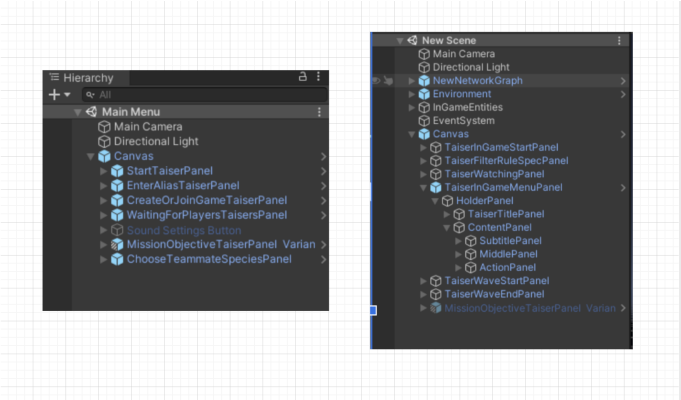

Fig. 4. Project structures of two different scenes of T2.

D. Data storage

Data are stored as CSV files in a filesystem on the server. When the subject completes the final wave of the session, a CSV file with all the data is created and stored on the server. CSV files are saved as the alias name followed by time and date. An Admin can only access those files which are stored in the specific URL. When the T2 is loaded, it reads the file with all the parameters and loads the parameters to the game. An admin can update the 'Parameter.csv' file by updating the parameters from the admin dashboard.

Name	Last modified	Size	Description
Parent Directory		-	
Parameters.csv	2022-12-25 17:54	466	
Raul_12_5_2022_9_51_28_PM.csv	2022-12-05 13:51	4.1K	
aa_12_5_2022_1_42_02_AM.csv	2022-12-04 17:42	17K	
aa_12_26_2022_12_56_37_AM.csv	2022-12-25 16:56	1.9K	
aaa1_11_27_2022_9_24_26_PM.csv	2022-11-27 13:24	5.5K	
aaa_11_27_2022_9_04_35_PM.csv	2022-11-27 13:04	5.9K	
aaa_12_6_2022_11_48_59_PM.csv	2022-12-06 15:48	1.8K	
aabbcc_12_5_2022_9_15_49_PM.csv	2022-12-05 13:15	4.9K	
aacc_12_2_2022_2_40_58_AM.csv	2022-12-01 18:41	429	
aacc_12_2_2022_2_40_59_AM.csv	2022-12-01 18:41	429	
aacc_12_2_2022_2_41_00_AM.csv	2022-12-01 18:41	429	
abc_12_9_2022_12_53_06_AM.csv	2022-12-08 16:53	1.3K	
acdc_11_27_2022_10_10_05_PM.csv	2022-11-27 14:10	5.5K	
sajal_test_12_9_2022_2_42_01_AM.csv	2022-12-08 18:42	1.7K	
sjl.csv	2022-12-06 15:57	1.3K	
sjl_11_30_2022_7_15_45_PM.csv	2022-11-30 11:15	44K	

Apache/2.4.41 (Ubuntu) Server at www.cse.unr.edu Port 443

Fig. 5. File storage of T2 in the server.

E. Testing

No third parties were used for testing tools or libraries. A group of computer science students performs manual testing every time before the actual study.

F. Deployment

The Unity WebGL build files of Unity and C# project is built from Unity manually and the build folder is pushed to the Linux server on a specific folder.

III. Conclusion

We have presented the software engineering design principle of T2. By breaking all the engineering aspects, we have created a web-based software simulation that collects the user data for Human behavior when humans and AI are teammates.

Additionally, which provides high performance and is able to approach efficient run-time speed. From the analysis of the development, we have created a platform for the Department of Psychology, to study and research human behavior when humans and AI are teammates. Therefore, the system can be used by more than fifty subjects at the same time and collect the data for the study.

To further improve this system, we have to enhance a few UI/UX features such that we prove limited freedom for the user while in the game. Likewise, the performance and the experience of the system can be improved by updating the life cycle method of the instance.

Acknowledgment

This work was funded by IUSE.