International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

REALM OF AUG MATRIX

[1]Dr.S. Mohandoss, [2]Thaya Govzig.P, [3]Melgibson Kawin Kumar.J [4]Ravuri Shanmukha, [5]E.R.Ramesh, [6]E.Durga Nandini

Cyber Forensics And Information Security
Dr. M.G.R. Educational and Research Institute,Chennai, India
[1]thaya.govzig2101@gmail.com, [2]melgibsonkawinkumar@gmail.com, [3]d37ravurishanmukha@gmail.com

ABSTRACT:

Our cybersecurity gamification website is designed to make learning and practicing cybersecurity skills more fun and engaging. The platform offers interactive games and challenges that cover basic cybersecurity topics and best practices. Users can progress through various levels and earn rewards as they learn and demonstrate their skills. The platform also includes educational resources and guidance to help users understand their understanding of online security. By gamifying cybersecurity education, we hope to make it more accessible and engaging to a wider audience, ultimately helping to create a safer environment.

KeyWord: cybersecurity, game theory,optimization, virtual reality

Introduction :

In today's digital age, cybersecurity has become a major concern for businesses, governments and individuals. Cybersecurity is the practice of protecting electronic devices, systems, and networks from theft, damage, or inaccessibility. As the number of cyber threats continues to increase, the need for cybersecurity experts also increases.In this case, cybersecurity games using Unity can be a fun and engaging way to educate people about the importance of cybersecurity. Cyber security. Unity is a popular game engine that allows developers to create 2D and 3D games for multiple platforms such as desktop, mobile and console. With its intuitive and powerful features, Unity is a great choice for creating games that deliver cybersecurity content. Cybersecurity games can be designed to test a variety of cyber threats such as phishing, malware, ransomware and social engineering. Games may also include different scenarios where players must identify and mitigate cyber threats. By playing the game, players can learn online best practices such as using strong passwords, updating software, and avoiding suspicious emails.The game is suitable for students, professionals and casual players as it can be designed for different ages and skill levels. The game can also be combined with online leaderboards and rewards to encourage players to compete and learn from each other.The game will have two levels. The first level is about general gaming, the second level is about cybersecurity. In the second level we will see some things related to cyber security with or without questions Each level will have a time limit and the player must complete the level within the specified time. Players will receive points when they complete each level and lose points when they fail a level or are subject to a cyber attack.

Requirement :

Needs analysis ·:

- Game mechanics: Game mechanics should be designed to simulate various online threats such as phishing, malware, ransomware and social engineering. The game will also feature different scenarios where players must identify and mitigate cyber threats.
- Player Interface: The player interface should be user-friendly and easy to understand. It should contain instructions explaining the game, objectives and management. The interface should give players feedback on their progress and performance.
- Graphics and Sound: Graphics and sound should be attractive and immersive,draw the player into the game. Games can be created in 2D or 3D, depending on the target audience.
- Multi-Platform Compatibility: The game must be compatible with multiple platforms such as desktop, mobile devices and consoles. It also needs to be optimized for different sizes and resolutions.
- Security Measures: Games should be designed in accordance with cybersecurity best practices, such as encryption, secure data storage, and protection against hacking and data exfiltration
- Leaderboards and Rewards: The game requires a system to track and display scores and progress. It should also provide rewards and incentives that encourage players to compete and learn from each other.
- Testing and Quality Assurance: The game must be thoroughly tested to ensure it is free from bugs and glitches Performance and compatibility should be tested on various platforms.

- Accessibility: Games should be made accessible to people with disabilities. It should have options such as adjustable text size, color contrast, audio description.
- Education: Games should be designed to educate players on cybersecurity best practices and increase awareness of cyber threats. It should also provide players with tips and resources to improve their cybersecurity skills.
- Special Information: Special Information is the process of interpreting and recording functional and non-functional information about the system. Here are more detailed features for the

Cyber Security Game using Unity:

Feature Requirements:

1. The game should simulate various online threats such as phishing, malware, ransomware and social engineering.
2. The game should include different situations where players must identify and mitigate cyber threats.
3. Games should provide players with feedback on their progress and performance.
4. Games need to be optimized for different platforms such as desktops, mobile devices and consoles.
5. The game must have a system to track and display player scores and progress. 6. Games should provide rewards and incentives that encourage players to compete and learn from each other. 7. The game needs to be thoroughly tested to ensure there are no bugs and glitches

Non-functional requirements:

1. The player interface should be user-friendly and easy to understand.
2. Graphics and audio should be engaging and immersive.
3. Games must follow cybersecurity best practices such as encryption, secure data storage, and prevent hacking and data leakage.
4. The game must be suitable for disabled people.
5. Games should be designed to educate players on cybersecurity best practices and
6. increase awareness of cyber threats.
7. The game should provide players with tips and resources to improve their cybersecurity skills.
8. The design of the game should provide players with a fun and engaging experience..

OBJECTIVES :

- To revolutionize education in the modern era.
- To make education easier and simpler.
- An innovative creation which relates with the education.

DESIGN AND IMPLEMENTATION :

Step 1: Open the Dedication's Integrated Development Environment (IDE)
- Start by entering the Dedication where development will occur.
- Launch an integrated development environment (IDE), your platform for writing, editing, and troubleshooting.
-This tool can be a tool like Visual Studio, Eclipse or any other popular IDE.

Step 2: Check the IDE and open Visual Studio Code (VS Code)
- Make sure the IDE is working properly.
- Open Visual Studio Code (VS Code), a lightweight, versatile code editor.
-Make sure it is properly configured to support the development environment

Step 3: Check the Augmatrix coding suite in VS Code
- In VS Code, check the configuration and correlation between coding suites required by Augmatrix development
-This may include libraries, extensions, or plug-ins specifically designed for virtual reality or matrix-related work.

Step 4: Consider Game Development with Sharing
-Consider Share Environment, a powerful game development platform.
- Make sure Unity is installed correctly and configured for gamemode development.
- Ensure that appropriate resources, scripts and dependencies are available for Augmatrix integration.

Step 5: Connect the VR device to the mounting engine
- Physically connect the virtual hardware device (VR) to the body.
- In Unity, configure settings to create connection to VR hardware.
-This includes introducing VR devices to use, setting up graphics, and connecting with Augmatrix functionality.

Step 6: Complete the game module in VR hardware setup
-Create a unified experience by completing the game module in Unity.
- Check if there are any errors or problems during testing.
- Make sure Augmatrix functionality works as expected in VR.

Step 7: End User Experience with Augmatrix
- Once the connection between the VR hardware and Unity is established, the end user can participate in the Augmatrix experience. - List additional steps or considerations for users to use Augmatrix to its full potential.
- Provide information or instructions to users to ensure that there are no problems in use.

RESULT :

- The game mechanics and objectives: Before you begin developing your gamification platform, you should have a clear idea of what you want to achieve with it. What are the learning goals? What game mechanics will you employ to keep the players interested? Define the rules, scoring system, and feedback mechanisms to keep the players engaged. Following cybersecurity topics to cover: Depending on your target audience, you may want to concentrate on various cybersecurity topics. For example, if you're creating a game for
- beginners, you might want to include basic concepts like password security, phishing, and malware. If you're creating a game for more advanced users, you might want to include topics like networking.
- This is a cybersecurity-based game which is made with the help of the unity game engine to teach people the concepts related with the cybersecurity. By this game people get to know what is cybersecurity, and people get a clarity on what is cybersecurity and how they are provoked and how they can be prevented properly. This can be easily influenced by the kids to adults and give a broad spectrum on the topic cybersecurity. Many may not have knowledge on what is cyber and cyber crimes and this is a platform where they are totally explained as a game.
- In this game we particularly covering topics which is totally related with the cybersecurity . and the few topics which are covered in this game are “PHISHING,SQL INJECTION ”and other topics .we used unity particularly in this game because unity is a game engine which is a best option to construct a gamin platform with a minimal load of work as compared to other gaming engine. In this game we implemented few ideologies like pixelated animation which is used to move the character and when it hits an obstacle that is present in the path then automatically pops up with an concept of the cyber related topics

CONCLUSION :

CYBER REALM game is used to simulate various cyber threats such as phishing, malware, ransomeware, and social engineering. In this we included various scenarios where player have to identify and mitigate cyber threats. Players can also learn about cyber security best pratices such us using strong password, updating software, and avoiding suspicious emails. This game is being invented for the awareness to the people such as kids to adults. This is to give a brief about the concepts of cybersecurity in a detailed manner in this game. It is the supplemented way to teach people about cybersecurity. Hence, we conclude that this game helps people to know about cyber and cyber related crimes

REFERENCES :

[1] Alla Levin, Tips for Optimizing an Online Gaming Experience, October 23, 2020
[2] Yuan Qing, Research and Implementation of H.265-based Video Rapid Codec, 2022 Int.
Conf. Net. Inf. Sys. Com. 02
[3] Bajovic, Mirjana. Violent Video Gaming and Moral Reasoning in Adolescents: Is
Therean Association? 2013 Edu. Med. Int. 50, 177–191.
[4] Christopher P. Barlett, Craig A. Anderson and Edward L. Swing. Video Game
EffectsConfirmed,
Suspected, and Speculative. 2008 Sim. Gam., 40. 377–403.
[5] Engelhardt, Christopher R., et al. This Is Your Brain on Violent Video Games:
NeuralDesensitization to Violence Predicts Increased Aggression Following Violent
Video Game Exposure. 2011, J. Exp. Soc. Psy., 47, 1033-1036.
[6]. Sedio, M.Z. (2021). Exploring e-tutors teaching of the design process as content

knowledge in an Open and Distance eLearning environment. Journal for the Education of Gifted Young Scientists, 9(4), 329-338

[7]. JAWAD ALSHBOUL1, GHANIM HUSSEIN ALI AHMED, ERIKA BAKSA-VARGA (2021) Semantic Modeling for Learning Materials in Etutor system.

[8]. Sheena Banks, Brigitte Denis, Uno Fors, Sebastien Pirotte (2014) Staff Development andE-Tutors Training

[9]. Aliakbari, M., & Hassen, Q. K. (2022). The Expectations and Reality of E-Learning. Mediterranean Journal of Social & Behavioural Research, 6(2), 61-66