Gamification by Students: An effective approach to cyber security concept learning

Sneha Thombre[1] and Makarand Velankar[2].

[1, 2] *MKSSS'S Cummins College of Engineering for women, Pune, Maharashtra, India*

Abstract— **The young (millennial) learners are not particularly motivated only by traditional classroom-based, one-way presentation/ lecture-based approaches as they are exposed to digital lives. Furthermore, in an outcome-based education system, all features of teaching focus on course outcomes. Therefore, the teachers face the challenge of student engagement. The work in this paper is regarding the active learning method for the final year students of the 'Information and Cyber Security' course. In this activity, the students design (in a group of 2) and build the game using the software platform of their choice. The game is built around the CIA triad (privacy, integrity. and availability), network security concepts and protocols. After designing and building the prototype of the game, the students for assessment and feedback play the game with their class mates and the faculty members. Then classmates and teachers give scores for each core drive on the Octalysis tool. This helps student game designers to improve the weak core. Octalysis is a gamification framework designed as an octagon shaped with 8 core drivers representing each side. The entire exercise is stimulating and motivates the students as indicated in their feedback of the students (68% of students rated excellent). Gamification by students proved to enhance student learning by promoting critical thinking and problem-solving skills, as evident from the assessment. Finally, course coordinator evaluates the game using rubrics that were shared with students beforehand. The evaluation rubric focuses on the title of the game, content, creativity, rules, instructions of the game, and cooperative efforts. Game design and implementation by students activity proves that the greatest benefit is that the maximum learning happens in the design process (for game designers) compared to players. Further, the students also learn to work in groups and solve problems. Furthermore, the most significant of the entire activity is learning of cyber security concepts and protocols in a fun way.**

***Keywords*—Active learning, Game design, Octalysis framework, assessment, evaluation and cyber security**

I. INTRODUCTION

THE Internet has revolutionized every aspect of human life and human business like the way we work, travel, socialize and even the way we learn and educate According to NASSCOM reports (Figure 1) indicates the Internet penetration In India from 2007 to 2021. Most aspects are technology-based and technology has made our era a digital era therefore, increased cyber security concerns. The increased pace of employment in the IT industry is indicated from Figure 2. In India 'Digital India' programs have made technology accessible to the common man and therefore ICT has changed the teaching and learning paradigms in the education domain. This is an external process where the digitalization of teaching and learning is influenced by government and international trends by the All India survey reports on Higher Education by Ministry of Education, GoI [2022]. Contrary, the use of digital technology for teaching and learning by the faculty members in their classrooms is an internal process. The role of the teacher is to take initiative and encourage learners. The teachers have to use active learning methods to engage students in the digital era.

Blended learning also helps to augment traditional learning. For high engagement and learning in the unlimited information era, the game-based learning approach for cyber security is being investigated in this research paper. The innovative aspects is students design and implement game rather than faculty member designing the game for students. The students need to understand the skill of the adversary's thinking to better understand cyber-attacks and their effective defenses. The novelty in this gamification is the games are designed and built are by the students for the students. The faculty is observer and does not assist in game design process. Student game designers lead discussions and problem solving strategies. The premise why students are involved for game design is that: when a game is created the greatest benefit is for the students who were engaged in the game design process and not to the players of the game. Secondly, game design and implementation is a collaborative process. From cyber security aspect game design by students facilitates knowledge construction, invention and reflection.

In literature, game-based learning is an accepted method of learning today (Boopathi K., et al., (2015), Yasin A. et al., [2018], Yasin A. et al., [2019], Hart G et al., [2020], Hwang G. et al., [2014]) but games were not designed by students. Games generally are played for fun, exceeding the opponent, accepting new challenges, etc. However, recently serious games are emerging for learning too. To achieve intended objectives for learning cyber security and to stimulate the interest in the cyber security course game-based learning was introduced in the final year undergraduate course of Information and Cyber Security.

The focus of this research work was to increase the engagement and participation of students in cyber security course. The methodology is game design and game implementation by the students. The game design exercise is integrated to make student designers understand the pertinent concepts like cyber security awareness, practical skill acquisition, strategy to protect assets from attackers, types of

attacks, important concepts like digital signatures, digital certificates, to generate interest in cyber security etc. A group of 2 students designed a game. Game designing and playing the game are highly engaging and students learn by practicing instead of knowing. Problem solving and increased knowledge content are natural outcomes of game based learning. Assessment and evaluation are both carried out. Assessment is an ongoing, positive process which provides feedback for improvement. It is carried by Octalysis framework. The analysis is presented in the results and discussion section. Evaluation is judgmental, applied against standard (rubrics) shows shortfalls and provides closure for the exercise.

The paper is divided into the following sections: after the first section of Introduction, a brief literature review of game-based learning for cyber security courses is carried out. Further, the methodology is discussed. Next, the results and discussions are presented followed by conclusions.

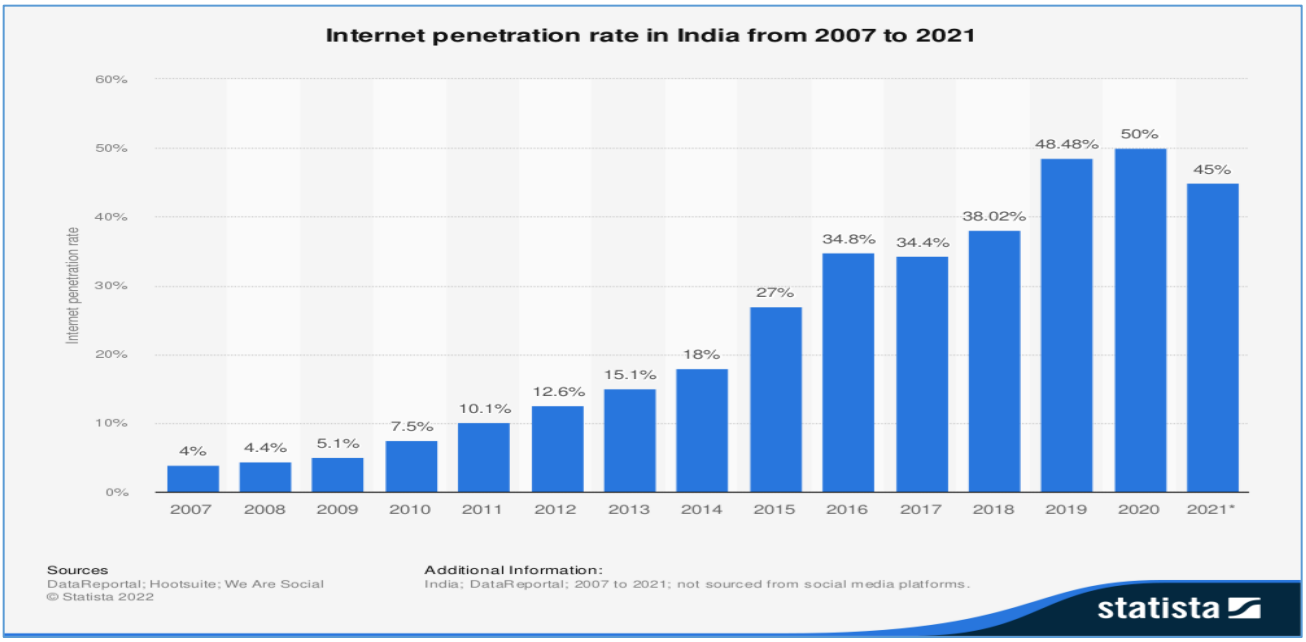

Figure 1. Internet Penetration rate in India

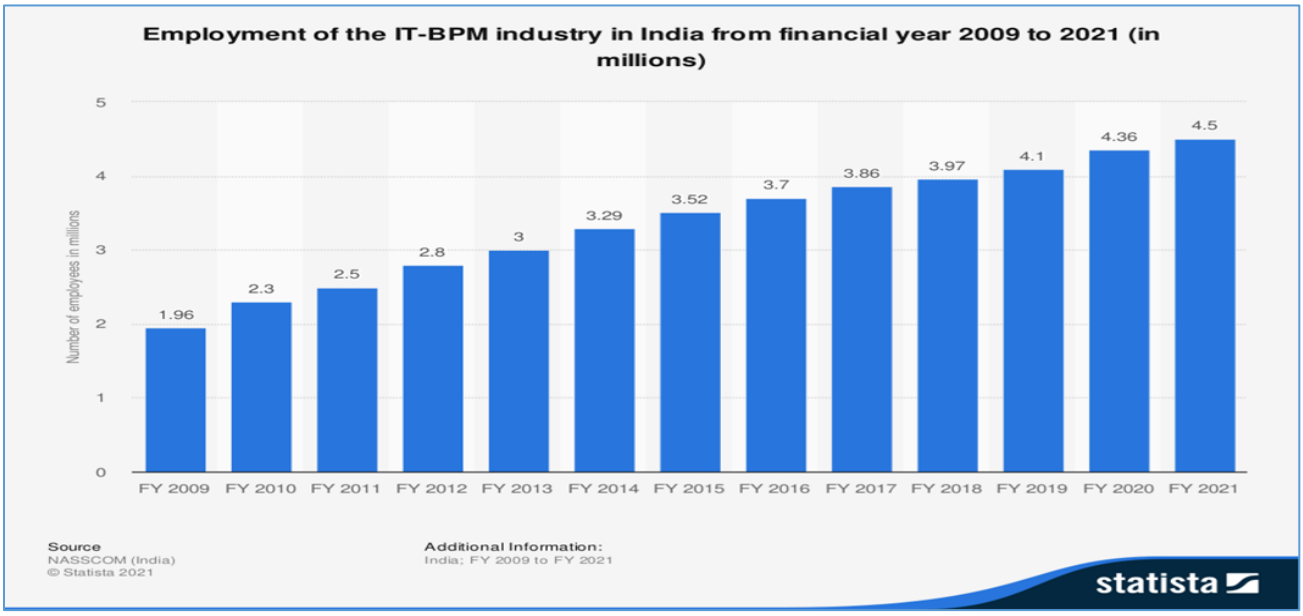

Figure 2. Employment of the IT-BPM Industry in India

II. LITERATURE SURVEY

The mechanism of game-based learning is new approach adopted by many instructors for enhancing the learning process of students. Game designing is a complex activity. Some research findings indicate that game design by students improve their attitude towards subject content, increased intrinsic motivation, metacognition, purposeful thinking constant decision making to troubleshoot and solve challenges as they emerge. (Hwang G. et al., [2014], Bentley T. [2015], Akcaoglu M. [2016]) Overall game design provides students with ample opportunities to formulate complex problems for the players to solve. Students get joy to create a meaningful product thereby this activity stands at the top level of revised Bloom's taxonomy.

Van Steen et al., [2021] focuses on the process of designing a game where Perceived Usefulness (PU) (Students inherently trust the learning happening) and Confidence (CO) (trust in the teacher and in his knowledge). The author argues that PU and CO are the pertinent factors that increase the perception of students towards learning cyber security cases. Malon M et al., [2021] distinguish between cyber security and non-cyber security game. Authors infer that that the cyber security games resulted in higher self-reported scores on attitudes, aware full behavioral control and intentions compared non-cyber security games.

Sharif K. H et al., [2020] conclude that the gamified learning experience for cyber security education is designed to provide learners with knowledge, comprehension and methods required to solve regular problems. Adams M et al., [2015] infer gamification as the best technique to create security awareness. The authors also provide recommendations to increase the effects of designing games. Wolfenden, B. et al., [2019] combined perspectives of entrepreneurial and gamification to develop skills for cyber security defense. Multiple scenarios for attack and defense were created to enhance learning. To understand timeliness and to design equilibrium between defense and offense security mechanisms the 'game of protection' is designed. Authors infer that now is the time for CISCOs and business leaders to reach for a new cyber security manual – one that support gamification in cyber security Y. K Chou et al, [2016]. Yu-Kai Chou actually proposed that Gamification is a design process which is human focused rather than function or system focused and the entire emphasis is on motivation.

Chou Y. [2013 and 2020] defined 'Gamification as the craft of deriving all the fun and engaging elements found in games and applying them to real-world or productive activities. Chou further elaborates that in general the systems approach is followed to get things done quickly as systems are designed for completing the job as quickly as possible. In reality, Octalysis framework is human-focused. Humans tend to have reasons to approach and do things, humans have feelings and insecurities and therefore games if designed human focused can achieve maximum engagement and participation with fun. The results of this work indicate maximum learning happens in human focused systems as optimized motivation and engagement is assured in human focused systems.

The Octalysis framework is human focused and based on Maslow's hierarchy of needs (Figure 3). Y. Chou has designed an Octalysis gamification framework as an octagon shaped with 8 core drives representing each side (Figure. 4).

Figure 3: Maslow's hierarchy of needs.
Source(https://octalysisgroup.com/octalysis-the-gamification-framework-backed-by-science/)

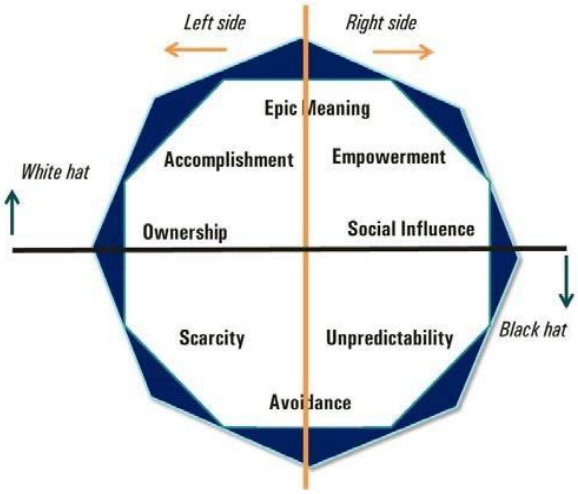

Figure 4: 8 Cores of Octalysis framework.
Source (https://yukaichou.com/gamification-examples/octalysis-complete-gamification-framework/)

The 8 cores of gamification are as given in the Octalysis framework devised by Yu-Kai Chou are as given below

1. Core Drive 1: Grand importance and mission is the need to contribute to something greater than ourselves.
2. Core Drive 2: Development and performance is about motivating people by making them feel they're improving and finishing successful championships.
3. Core Drive 3: Empowering creativity and feedback is that the core drive that motivates people to be

creative, try different permutations and methods, seek feedback and adapt.

4. Core Drive 4: Property and possessions is the primary core drive that motivates people to accumulate, improve, protect and acquire more of their possessions.
5. Core Drive 5: Social Influence and connection relates to activities motivated by other people's influence.
6. Core Drive 6: Scarcity and impatience make people want what they cannot have (e.g., because it isn't readily or easily available).
7. Core Drive 7: Unpredictability and curiosity is the willingness to explore the unknown and embrace opportunities.
8. Core Drive 8: Loss and Avoidance refers to motivating factors that help people avoid unwanted losses and situations.

Right brain and left brain indicate expression, creativity and analytical thinking respectively. The highest and bottom are black and white hats respectively. Black Hat drives motivation to move forward, while Black Hat has a drive associated with the negative urge to move forward.
To generate an Octalysis Score, players rate how well the subject being analysed is in each core drive, assigning a range from 0 to 10 based on their own insight, data, and knowledge, and assigning that number to square it to get the core value. In general, at least one of the above core drivers needs to be strong for a compelling and engaging game. To use Octalysis, one needs to identify all the game mechanics that appeal to each core drive and list them next to the Octagon's core drive. The octagon shrinks or expands, and the octagon shape reveals weaknesses in the game design. This is a self-evaluation method for games designed. One of the student-designed game octagons is shown in Appendix A. Each group of game designers and implementers have their own Octagon. This is the formative evaluation drive score. The octagon shape helps game designers improve their game according to the weaknesses represented by the octagon. A good way to get feedback during game design iterations helps students quickly understand design and implementation flaws
Therefore, To be truly engaging, the activity must be

1. It should be structured so that players can increase or decrease the difficulty according to their ability.
2. Allow the activity to be easily separated from other stimuli that may interfere with the player.
3. Have clear performance standards to let students know how well you're doing and how little you're doing poorly, and give specific feedback to tell them how well you're meeting the standards.
4. There is a wide range of challenges, and in some cases there are several qualitatively different ranges of challenges.

III. METHODOLOGY

Game design activity as indicated earlier is for the final year undergraduate students from the Department of Information Technology for the course Information and Cyber Security. The game design activity is part of their continuous internal assessment. Students are informed about the activity during the first session of the course. The game design is to be completed by a group of 2 students. Game design is a complex process.

Students will complete the following steps:

1. Brainstorm game ideas and come up with games that can be implemented despite technology limitations and other limitations.

2. Prototype the idea in a quick and dirty version of the game to identify problems and develop a better version of the game. This is the early stages of experimentation.

3. Test the game with their friends and ask for suggestions and feedback and use the gamification framework, an Octalysis tool.

4. Take suggestions and improve the prototype.

5. Play games with faculty, get feedback, and use the gamification framework, an Octalysis tool. Export the octagon and include it in report to be submitted to the instructor.

6. Write a full exercise report and submit it to the instructor.

7. Finally, for summative assessment, students are assessed against the rubrics previously communicated to them.

The evaluation of the entire game design exercise is carried out by the instructor. The evaluation rubric focuses on the game's title, content, creativity, rules, gameplay, and collaboration. (Rubrics is shared with students).

For formative assessment, the frequency of meetings with students during the gamification process was more informal. With the focus on the process, cyber security knowledge and creative gamification skills the game designed by students were evaluated as the main grading and is performed at the end of the exercise. Therefore,, assessment was focused on how learning was happening more of process oriented, diagnostic in nature and evaluation by the instructor thrusts on what students have learnt means more of product oriented.

The actual assignment shared to the students by the instructor with the discussion is as below:

Gamification Assignment:

Serious games aim to do more than entertain. Build a game to sensitize players and/or learn, network security concepts and protocols. Write the title of the game, the rules of the game, and any other guiding diagrams. Implement the game with available and known technology. The team size should be of 2 students and each team can play their designed game with the classmates, mentor/project guide or any faculty member of the institute to get scores on Octalysis framework as well as their comments/suggestions. This will help team designers to improve the game before final submission for evaluation. Then each team should document the game and submit a brief report. A rubric for evaluation is shared with all teams.

Use an Octalysis tool (https://yukaichou.com/octalysis-tool/) and export your Octagon in the report.

Some sample games

1. The McDonalds Game
2. Anti-Phishing Phil

3. The ReDistricting Game
4. 3rd World Farmer
5. Data Dealer
6. Diabetic Dog

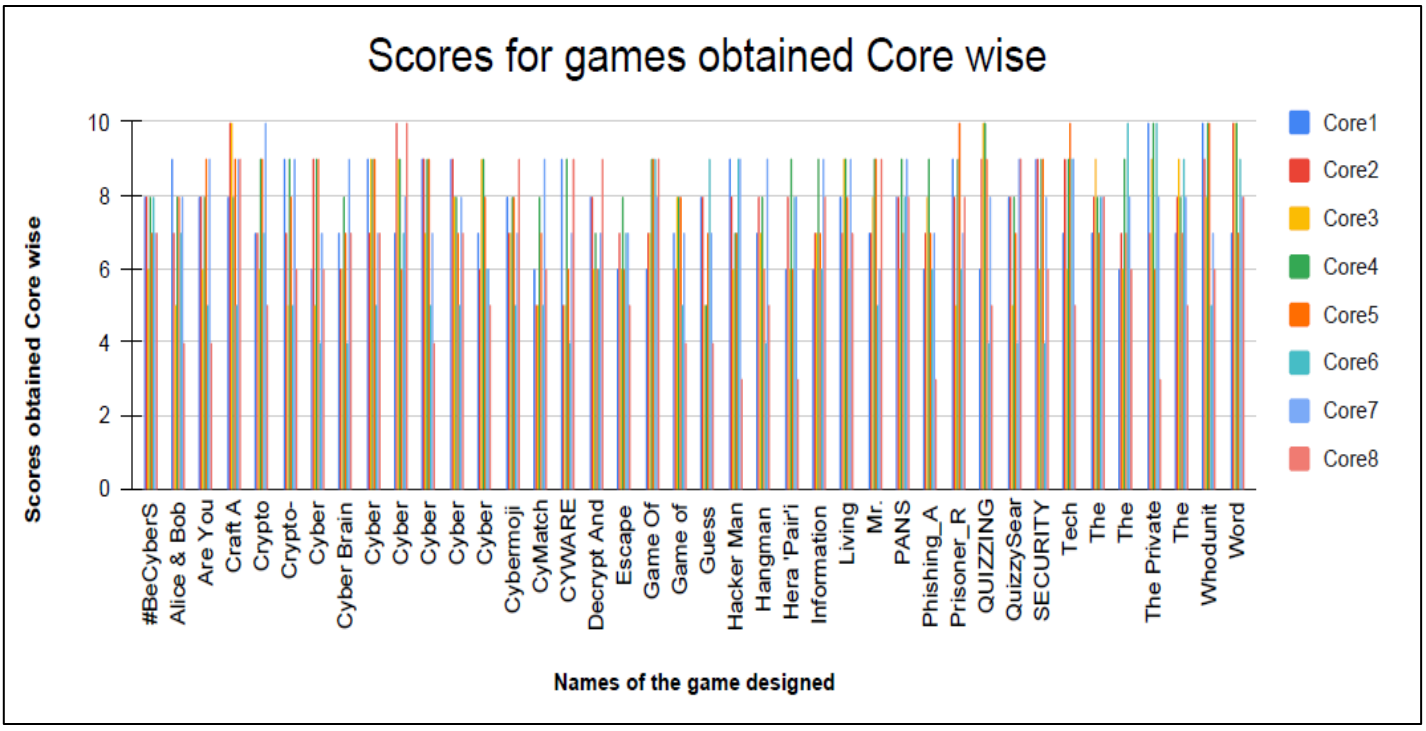

Figure 5: Scores of all the games indicated core wise

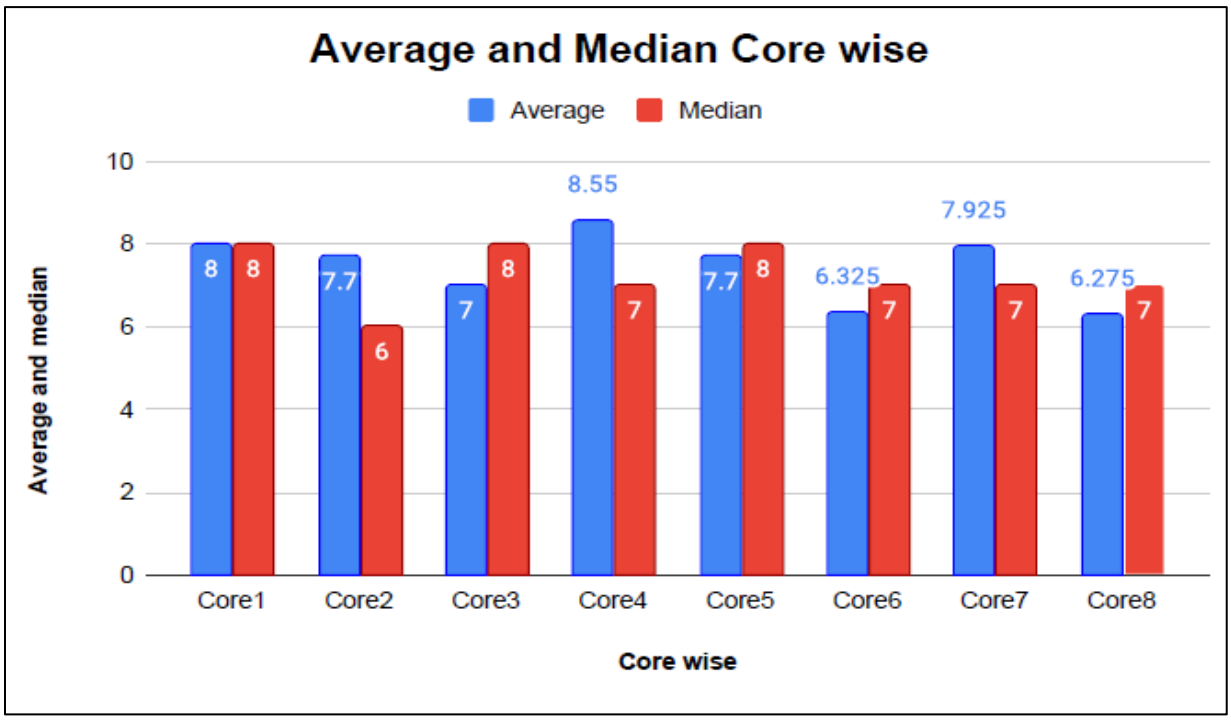

Figure 6: Average and Median values of all the games indicated core wise

IV. Results and Discussions

Firstly, the analysis and discussion about formative assessment. Regarding the formative assessment the students were good at Core 1 and Core 4 as indicated by the average and median values (see Figure 5 and Figure 6). It can be deduced that that the players were encouraged and

attracted students to play. This clearly infers that games if games designed by the students, then those games had the ability to make players devote time for the play willingly and give feedback to the game designers enthusiastically. Better scores for core 4 indicate that players had the feeling of ownership and that the players innately want to better it. This is significant because it the success of the designers of the game that make the players feel ownership. If designers and players are peers, the requirements of the game elements are better understood.

Figure 5 and Figure 6 indicate that for Core 6 and core 8 the scores were less comparatively. Core 6 is regarding the impatience and scarcity as the game element. The core indicates that players want something because they cannot have it. The dynamics of this game element is that players think about it daylong if they cannot have it. This aspect game student game designers could not get well compared to rest aspects. One more core where game designers students underperformed little was of Core 8 which talks of loss and avoidance. The avoidance of something bad happening is the foundation of this fundamental motivation says core 8. On a smaller scale, it can be to keep prior work from being lost. On a bigger scale, it can be to keep from having to declare that all you've done up until this point has been in vain since you're resigning. This Core Drive is also heavily utilized when possibilities are rapidly disappearing because players believe that if they don't act now, they will never again have the chance to act. Instructor made deliberate efforts for student game designers to make them understand Core 8 aspect of game design. Figure 7 shows one Octagon designed by students namely, Hacker Man. Similarly, every game designer had their Octagon indicating strengths and weaknesses of their designed game according to Octalysis framework. We used only Level 1 of the Octalysis framework as the student game designers are not experts.

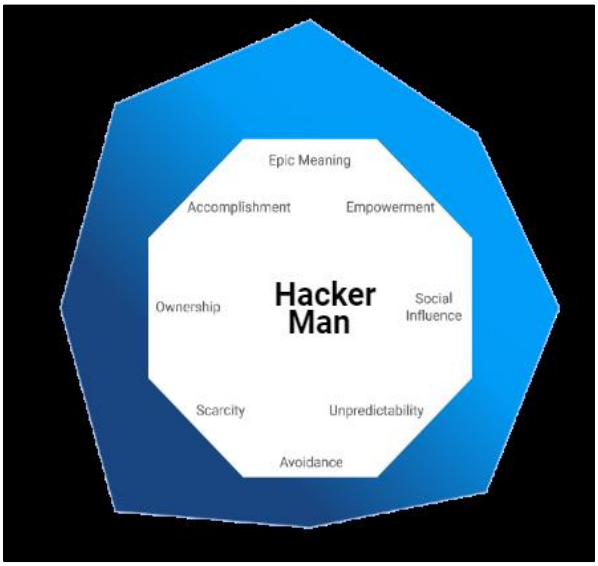

Figure 7: Sample Octagon for a game ‘Hacker Man’

Regarding evaluation, instructor evaluated the games based on the rubrics (see Appendix A).

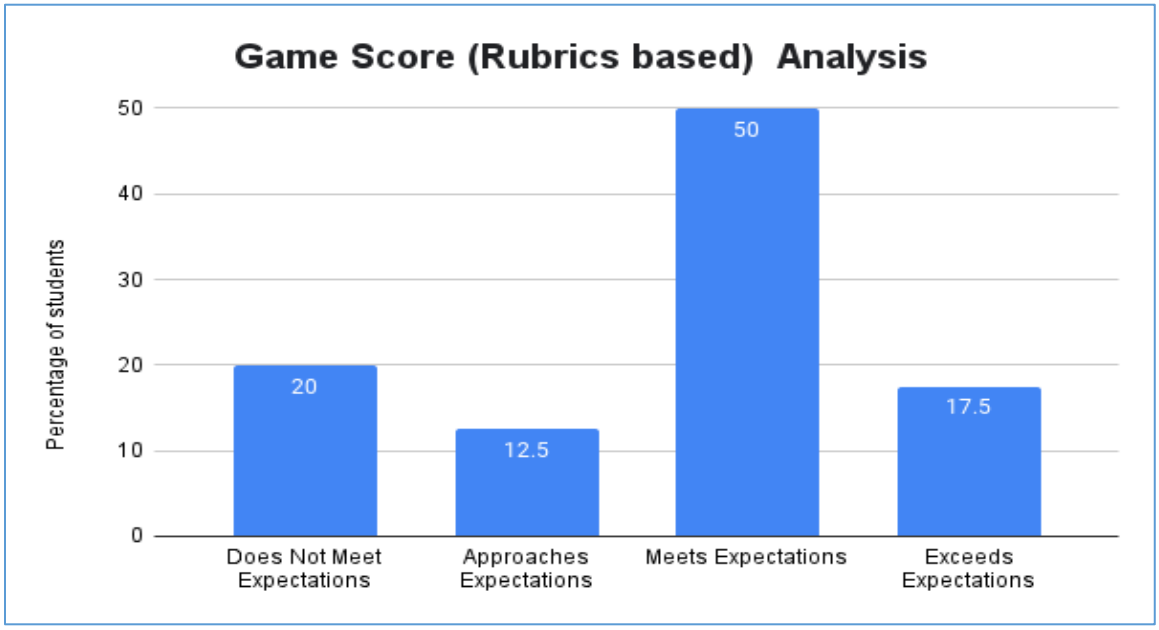

Figure 9: Rubric based evaluation score analysis of the designed games.

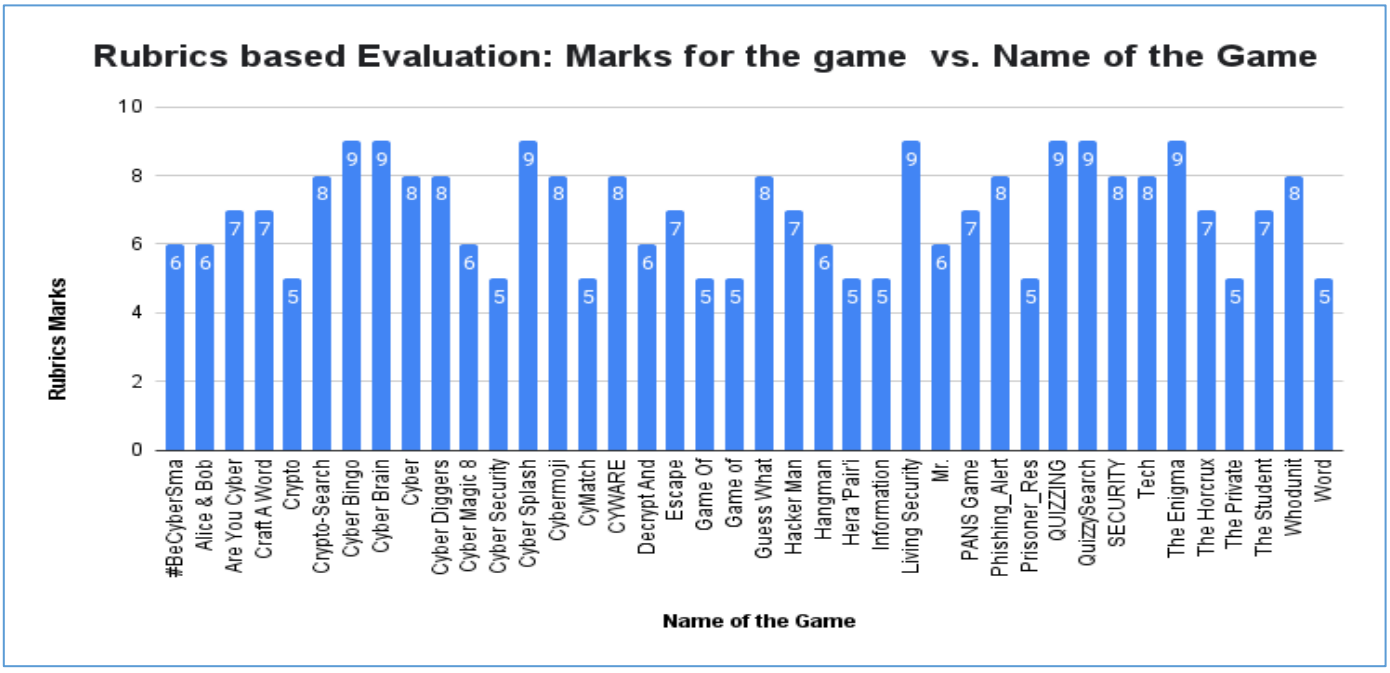

Figure 8: Game scores Rubrics based

The Figure 8 indicates the marks scored by each game and Figure 9 presents the analysis of the marks obtained. The analysis clearly indicate the increased participation, involvement in the game design exercise. Good scores indicate the game designers did good job despite the game were designed for the first time. Only 20% did not meet the the expectations but rest did very well. Overall, the game design exercise met the objectives of the activity as we clearly see increased motivation as all the students participated enthusiastically and improved the game with feedback. Creativity, content and cooperation among the students was excellent.

The feedback on the game design exercise from the concerned students infers those students enjoyed the exercise. The results are presented in Figure 10, Figure 11 and Figure 12.

1. Game design activity was motivating.

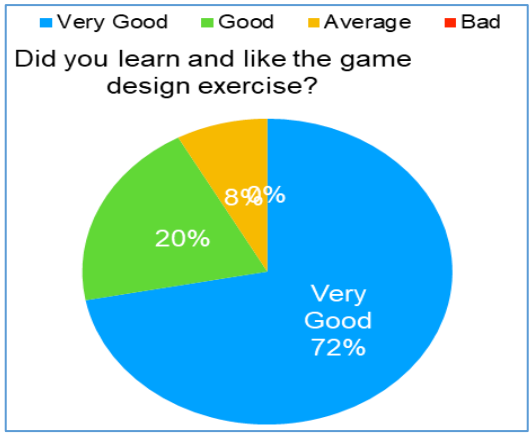

Figure 10: Student feedback on the game design activity

2. The game to be designed was for our class-mates (students). So, understanding the audience was easy.

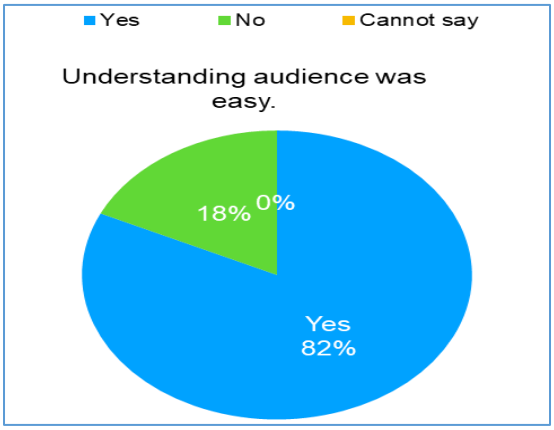

Figure 11: Student feedback on the game design activity

3. Is game designing creative?

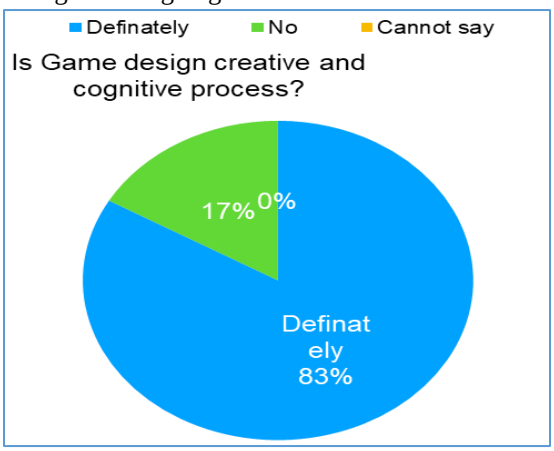

Figure 12: Student feedback on the game design activity

V. CONCLUSIONS

Gamification by students for students in an excellent active learning method for the course cybersecurity. The game design activity increased motivation for learning with fun. Game design is a concept and game implementation is execution. Students find game designing exciting as it requires different skills like creativity, problem solving skills, ability to work in teams, flexibility to make changes according to the feedback received, understanding the topic and concept of game design cybersecurity in our case. Cyber security is an apt course for learning cyber security concepts. Secondly, Octalysis is a best tool to the formative assessment game design activity. Octalysis framework is human focused and not only system based with the objective of increasing motivation. Though we used only level 1, further levels can be explored. The rubrics evaluation augmented the formative assessment. Further, exploration needs to be continued for using Octalysis tool. The results of the activity infer that the gamification approach with octagon analysis can be used to learn and explore concepts in different domains effectively. It helps in building design skills among students which is considered as the most sought higher order thinking skills as per revised bloom's taxonomy.

REFERENCES

All India survey on higher Education. 2022. *https://aishe.gov.in/aishe/gotoAisheReports*. online] Available<https://aishe.gov.in/aishe/home> [Accessed 2 January 2022].

Boopathi, K., Sreejith, S., & Bithin, A. (2015). Learning cyber-Security through gamification. *Indian Journal of Science and Technology, 8(7), 642-649.*

Yasin, A., Liu, L., Li, T., Wang, J., & Zowghi, D. (2018). Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG). *Information and Softwar Technology*, *95*, 179-200.

Yasin, A., Liu, L., Li, T., Fatima, R., & Jianmin, W. (2019). Improving software security awareness using a serious game. *IET Software*, *13*(2), 159-169.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, *95*, 101827.

Hwang, G. J., Hung, C. M., & Chen, N. S. (2014). Improving learning achievements, motivations and problem-solving skills through a peer assessment-based game development approach. *Educational technology research and development*, *62*(2), 129-145.

Bentley, T. M. (2015). *The game studio: Developing Literacy through the lens of game design* (Doctoral dissertation, Middle Tennessee State University).

Akcaoglu, M., & Bowman, N. D. (2016). Using instructor-led Facebook groups to enhance students' perceptions of course content. *Computers in Human Behavior*, *65*,582-590.

Van Steen, T., & Deeleman, J. R. (2021). Successful gamification of cybersecurity training. *Cyberpsychology, Behavior, and Social Networking*, *24*(9), 593-598.

Malone, M., Wang, Y., James, K., Anderegg, M., Werner, J., & Monrose, F. (2021, March). To gamify or not? On leaderboard effects, student engagement and learning outcomes in a cybersecurity intervention. In Proceedings of the 52nd ACM Technical Symposium on Computer Science Education (pp. 1135-1141).

Sharif, K. H., & Ameen, S. Y. (2020, December). *A review of security awareness approaches with special emphasis on gamification.* In 2020 International Conference on Advanced Science and Engineering (ICOASE) (pp. 151-156). IEEE.

Adams, M., & Makramalla, M. (2015). *Cybersecurity skills training: An attacker-centric gamified approach.* Technology Innovation Management Review, 5(1).

Wolfenden, B. (2019). *Gamification as a winning cyber security strategy.* Computer Fraud & Security, 2019(5), 9- 12.

Y.-K. Chou, *"Actionable gamification: Beyond points, badges, and leaderboards*," Octalysis Media, 1–151, 2016, doi: 10.1017/CBO9781107415324.004.

Y. Chou, Octalysis: Complete Gamification Framework – Yu-Kai Chou, 2013.

Y. Chou, Octalysis / Gamification Building, Developing Online Tool - by Yukai Chou, Dec. 2020.

Appendix A

ICS T1 GAME RUBRIC INSPIRED BY

BY HTTPS://WWW.TEACHERSPAYTEACHERS.COM/PRODUCT/GIFTED-EDUCATION-MATH-GAME-DESIGN-PROJECT-RUBRIC-485311

	Degree 1	Degree 2	Degree 3	Degree 4	Marks
Creativity	Little creativity used to make the game, informative or fun.	Some creativity used to make the game informer and fun.	Above average creativity used to make the game informer, appealing.	High level of creativity used to make the game informer, appealing.	
Content	Very little factual content.	Moderate level of information is presented and factual.	The above average level of information is presented and factual.	The high level of information presented is factual.	
Rules and Instructions	No written rules or instructions were provided.	Limited written rules and instructions were provided.	Sufficient written rules and instructions were provided.	Well- developed, easy-to-follow written rules and instructions were provided.	
Cooperative Effort	The student did not work cooperatively with the team.	Student contributed limited cooperative effort on the Game.	Student contributed above average cooperative effort on the Game.	Student contributed a high level of cooperative effort on the Game.	
				Total	

Teacher	Student Self-Assessment