# Cybersecurity Awareness Through Interactive Learning Using the CyberVigilance Game

**Mike Wa Nkongolo, Thami Sithole and Jahrad Sewnath**
University of Pretoria, Department of Informatics, South Africa

Mike.wankongolo@up.ac.za
u22835416@tuks.co.za
u21442534@tuks.co.za

**Abstract:** Cybersecurity has become increasingly important in today's digital landscape, with end users bearing a major duty to ensure the security of computer systems. A significant percent of data breaches are associated with human involvement, highlighting the crucial role individuals play in cybersecurity and the necessity of developing practical solutions to mitigate security risks associated with human factors. Traditional training approaches often fail to adequately address cybersecurity-related human errors due to low engagement levels and lack of interactivity. To address these shortcomings, this research introduces '*CyberVigilance*,' an instructional cybersecurity game designed for students. It is implemented as an interactive educational game to teach cybersecurity principles. The game contributes to cybersecurity awareness by offering students an engaging, hands-on learning experience. The feedback and scoring mechanisms within the game reinforce the importance of cybersecurity awareness, motivating students to apply what they have learned in practical contexts. Using a multi-agent system (MAS), CyberVigilance integrates cards and feedback to represent various cybersecurity scenarios in a competitive game where students act as defenders against computer-simulated attacks. Students earn points by selecting cards linked to cybersecurity awareness, which enhances their decision-making skills and prepares them for real-world cybersecurity threats. Most importantly, the game captures data on students' performance, which is then analyzed to assess the effectiveness of the MAS in predicting and classifying their actions using machine learning (ML). This ML-driven approach aims to provide insights into students' decision-making patterns, identify areas needing improvement, and adaptively enhance training by tailoring feedback to strengthen cybersecurity skills.

**Keywords:** Cybersecurity awareness, Human factors, Interactive learning, Multi-Agent systems, Serious games, Machine learning analysis

## 1. Introduction

Cybersecurity has become increasingly important in today's digital landscape as the end user bears the major duty of guaranteeing the security of computer systems. A substantial percent of data breaches are associated with human involvement (Jerry-Egemba, 2024). Many cybersecurity incidents are caused by human-related issues such as mistakes, misuse of privileged accounts, use of stolen credentials, and social engineering techniques. This highlights the crucial role that people play in cybersecurity and the necessity of developing practical solutions to address and lower security risks associated with human factors (Jerry-Egemba, 2024; Bothos and Vlachos, 2024). Conventional training approaches frequently fail to adequately address and mitigate cybersecurity-related human errors and losses for a variety of reasons (Jerry-Egemba, 2024; Ozkan-Ozay et al., 2024). For instance, if the training is thought to be boring or unnecessary, negative views around cybersecurity may also unintentionally grow (Ozkan-Ozay et al., 2024; Jerry-Egemba, 2024; Bothos and Vlachos, 2024). Therefore, adopting customized training methods, such as multi-agent systems (MAS), can help integrate real-world scenarios to foster active cybersecurity learning (Oltramari et al., 2014; Tolks et al., 2024). MAS design can be used to replicate realistic cybersecurity scenarios by creating serious games that serve as an engaging alternative to traditional training methods. This approach has also been applied in various other training domains, such as computer programming, conflict resolution (Gil Ruiz, 2024), and health promotion (Pérez-Jorge et al., 2024), to incentivize behavioral changes and enhance situational awareness. However, the use of MASs in the cybersecurity landscape is very new. The research motivation is centered on addressing the critical role of human factors in cybersecurity and the shortcomings of traditional training methods in reducing human-related errors. With data breaches often stemming from human mistakes, misuse, and social engineering, there is a need for more effective solutions to improve cybersecurity awareness. Traditional training approaches are frequently disengaging or insufficient in promoting active learning. This research aims to tackle these challenges by introducing *CyberVigilance*, an interactive game that combines MAS and machine learning (ML) to study and enhance students' cybersecurity decision-making skills. The game provides a dynamic, hands-on learning experience, where students engage with real-world cybersecurity scenarios to reinforce their understanding of security practices. The game also uses ML to analyze and classify student actions by capturing data on player performance, thereby providing valuable insights into their decision-making patterns and helping to improve future training strategies. The motivation behind this research is to offer an engaging, effective, and data-driven

solution to enhance cybersecurity training and awareness for students. The research question is: *How does the CyberVigilance game enhance students' decision-making in cybersecurity, and how can ML be used to analyze and classify decision-making patterns to improve training outcomes?*

### 1.1 Related Works

Research studies on learning theories and cybersecurity education highlight various advantages and limitations. These limitations are discussed in Table 1. Behaviorism and connectivism were prominent in the studies by Scholefield and Shepherd (2019), Hassan et al. (2022), and Eltahir and Ahmed (2023). These studies highlight the development of security-awareness applications to create learning networks for practical business issues. They faced limitations in addressing gender disparities, incorporating work-integrated learning, and thoroughly investigating model frameworks (Table 1). Gemade (2022) demonstrated the effectiveness of gamification in teaching students, while Grobler et al. (2021) examined practical cybersecurity improvements, which were hindered by issues related to students' memory retention. Other studies explored diverse learning theories with various applications in cybersecurity. For instance, Gil Ruiz (2024) and Stojkovski (2022) found social constructivist approaches effective in motivating students, but struggled with generalisability and participant enrollment. Fagbule (2023) and Chowdhury et al. (2022) focused on social cognitive theory and personalized learning theory, noting awareness of knowledge gaps, yet faced challenges with participant opinions (Table 1). Lastly, studies by Sungkur (2020) on cognitive constructivism highlights algorithm robustness and mobile gaming adaptability. Existing research gaps are clearly outlined in Table 1 to situate our study within the current literature.

**Table 1: Learning theory in cybersecurity games**

| Author | Learning Theory | Advantage | Limitation |
|---|---|---|---|
| **(Scholefield & Shepherd, 2019)** | Humanism | An application for security-awareness games. | Due to the absence of the participant questionnaire, gender disparities must be investigated. |
| **(Eltahir & Ahmed, 2023)** | Humanism | Developers can download both free and commercial components for their applications by using the MAS. | Viability and efficacy. |
| **(Hassan et al., 2022)** | Connectivism | Creating a learning network to solve any practical business issue by establishing links between concepts. | Aspects of the literature review prevents a thorough investigation of all possible pairings between model frameworks and learning objectives. |
| **(Gemade, 2022)** | ML | Gamification to supplement traditional teaching methods. | Research design, methodology, data collection technique, and the time frame. |
| **(Gil Ruiz, 2024)** | Constructivism | Bolster motivation, optimize learning, and enhance student abilities | Findings are difficult to generalize because of the tiny sample size. |
| **(Stojkovski, 2022)** | Constructivism | Affordable strategy that impacts the entire businesses, sectors. | Challenges in obtaining and enrolling a greater number of participants from the intended audience. |
| **(Fagbule, 2023)** | Cognitivism | People that receive training become aware of knowledge gaps. | The research design and approach employed to get results were modified. |
| **(Chowdhury et al., 2022)** | Humanism | It makes it simpler to identify and directly revise any component that might need to be changed. | The potential to ignore the opinions of minority participants and the absence of precise methodological frameworks. |
| **(Grobler et al., 2021)** | Constructivism | Looking into more practical ways to improve cybersecurity. | Memory loss when it comes to the use of passwords as security measures. |
| **(Asselman et al., 2018)** | Observational | e-learning makes it possible for students to access instructional materials efficiently. | Remote areas with limited ICT infrastructure. |
| **(Sungkur, 2020)** | Cognitivism & constructivism | Robust, and yielding consistent answers across a wide range of problems. | Conceptual model to be critically examined to ascertain its academic validity. |

| Author | Learning Theory | Advantage | Limitation |
|---|---|---|---|
| **This work** | Constructivism , cognitivism & ML | CyberVigilance gameplay data for cyber gaming analytics. | Generalizability. |

## 2. Methodology

In the CyberVigilance game, each participant is provided with 13 distinct cards that symbolize either attacking or defending strategies as shown in Table 2. The game begins with an empty board, and players alternate turns to place their cards, representing strategic decisions that reflect optimal or sub-optimal moves (Nkongolo, 2023; Nkongolo, 2024). The attacker starts the game, and a judging entity evaluates each move, awarding a point for the best strategic placement and a zero for less effective moves (Table 2). This format aims to replicate real-world cybersecurity scenarios, enhancing players' understanding of best practices through strategic thinking and decision-making (Nkongolo, 2024). The straightforward rules and turn-based nature of the game facilitate easy engagement, while the competitive element drives players to refine their strategies, balancing offense and defense to outmaneuver their opponents and achieve their goals. The CyberVigilance dataset is constructed by having various players participating in the game. The top players are then extracted from the scoreboard. This dataset includes their nicknames, scores, outcomes (winners), levels, and game times, which are all parsed and published.[1]

**Table 2: The player tokens, scores, and judge feedback**

| Attacker Cards | Defender Cards | Winner | Attacker Score | Defender Score | Judge Feedback |
|---|---|---|---|---|---|
| **Access** | Deny | Defender | 0 | 1 | Blocking/denying actions |
| **Phone** | Provide | Attacker | 1 | 0 | Information shared |
| **Click** | Backup | Attacker | 1 | 0 | Backup lost |
| **Chat** | Identify | Defender | 0 | 1 | Verification/identification |
| **Total** | | | 2 | 2 | Draw |

### 2.1 Improvement of the CyberVigilance Game

This study explores the research question through the CyberVigilance game, introduced in Nkongolo (2024) by (i) using ASP.NET, (ii) updating rules, and (iii) designing new cards generated by *Bing's AI* from textual descriptions (Figure 1). Card effects are deterministic, with randomness introduced only in the order of card placement by the attacker/computer program against the defender/students. Both players, with advanced and limited prior knowledge of cybersecurity, are introduced to the CyberVigilance cards through a brief description provided before the game starts (Figure 2). This description explains the purpose and function of each card, outlining how they relate to key cybersecurity principles (Figure 2). By presenting the digital cards in an easy-to-understand format, players gain a foundational understanding of how to use them during gameplay. This *pre-game* introduction ensures that even those with little prior knowledge can engage with the game effectively, making the learning process more accessible and interactive.

[1] https://www.kaggle.com/dsv/9480976

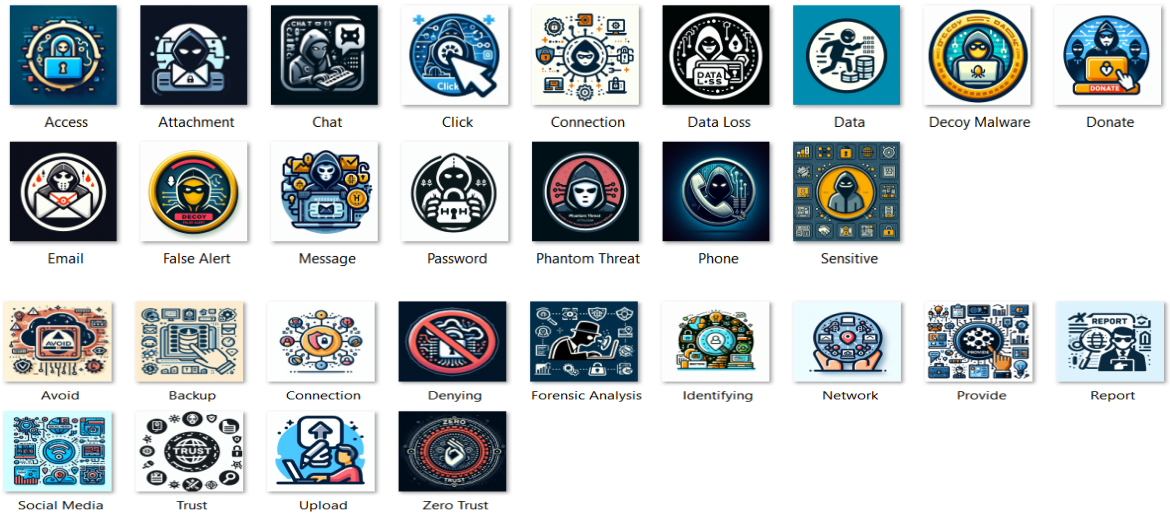


**Figure 1: The attacker and defender cards generated by Bing's AI (author's images)**

### 2.2 Dataset Creation

To create a dataset with various players, robust game states, and actions at each turn, the CyberVigilance scoreboard is scraped to retrieve data from the top players/students (Figure 3). This encompassed a range of players from beginners to experts. Subsequently, the research utilizes this scoreboard to gather the most recent games played by each student, formatted as csv files (Figure 3). Gameplays were excluded from the dataset if the student did not use the same nickname consistently. This constraint is crucial for analyzing individual player behavior. The final dataset contains 136 students who played the game 11 times, allowing for the analysis of their progression. Furthermore, CyberVigilance offers personalized feedback by analyzing selected cards with the game duration and outcome used to assess player proficiency levels (Figure 4).

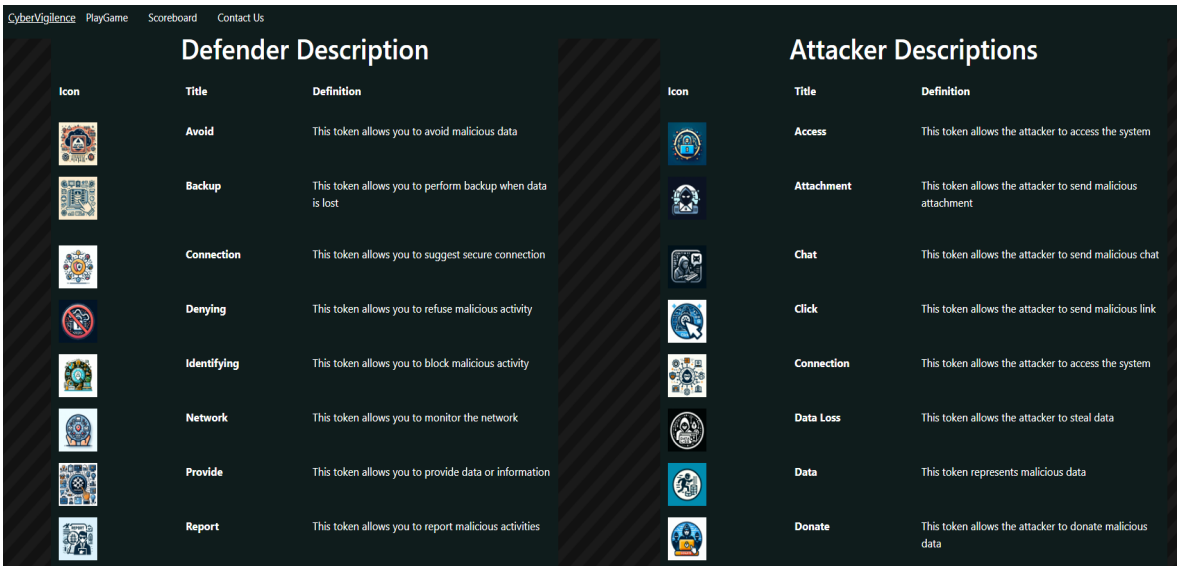


**Figure 2: Digital card's descriptions (author's images)**

### 2.3 Player Demographic Information

The target participants are computer science and information science students with diverse backgrounds and expertise levels, making them well-suited for evaluating the game. In addition, the study implements a condition where a participant (defender/student) achieves an expert level only if they defeat the computer program (attacker) within an adjustable time frame of 160 minutes. Students' gameplay information is retrieved using local storage and stored into a *csv* format (Figure 3).


**Figure 3: The CyberVigilance scoreboard (author's images)**

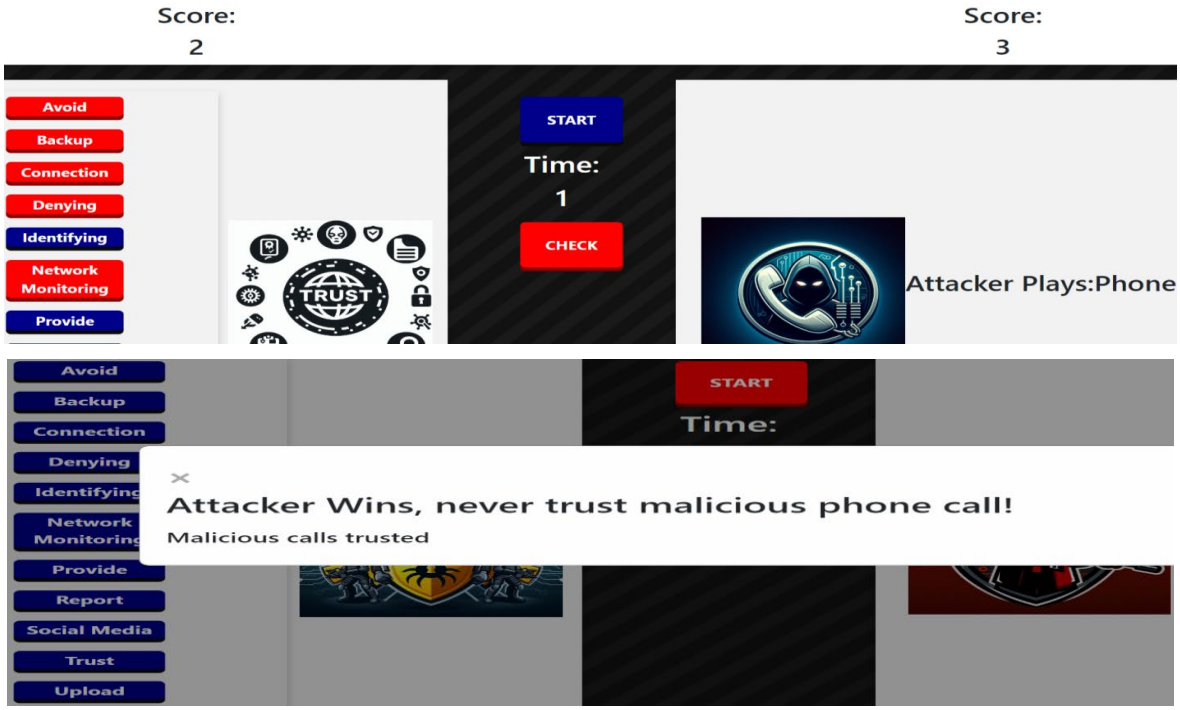


**Figure 4: Personalized feedback is given based on card selections: if the attacker picks the "*Phone*" card and the defender picks "*Provide*," the judge announces the attacker as the winner (author's images)**

Each entry in the resulting dataset corresponds to a single turn, containing the student's nickname, game outcome, and playtime (Figure 3). This process yielded 1,077 data points representing a balanced section of the dataset to study specific student's behavior and progression. The aggregated dataset is then split randomly into training (80%) and testing sets (20%). Lastly, the game's software requires a desktop or personal computer with a connected mouse and keyboard to enable gameplay.

### 2.4 Machine Learning for Player Identification

Lazy Predict is a Python library designed to simplify the initial stages of ML models evaluation by providing a fast, and automated way to generate and compare predictions from various models without extensive hyperparameter tuning (Galván et al. 2011). It is particularly useful for benchmarking multiple algorithms to determine which performs best on the CyberVigilance dataset for player identification, classification, and playstyles recognition.

## 3. Machine Learning Results

The ML results using Lazy Predict are presented in Figure 5 and Table 3. Among the best-performing models based on accuracy and F1-score, several algorithms achieved a perfect score of 100% in both metrics (Figure 6). While they all demonstrated exceptional performance, the time taken for training is a significant factor when choosing the best model (Galván et al. 2011), especially in practical scenarios where computational efficiency is essential (Table 3). Given these considerations, KNeighborsClassifier, RidgeClassifierCV, LogisticRegression, and LinearSVC stand out as the best choices due to their combination of perfect accuracy, F1-score, and minimal training time (Figure 5 and Table 3). These models not only provide top-notch performance but also ensure efficient use of computational resources, making them ideal for real-time applications and large-scale data processing.

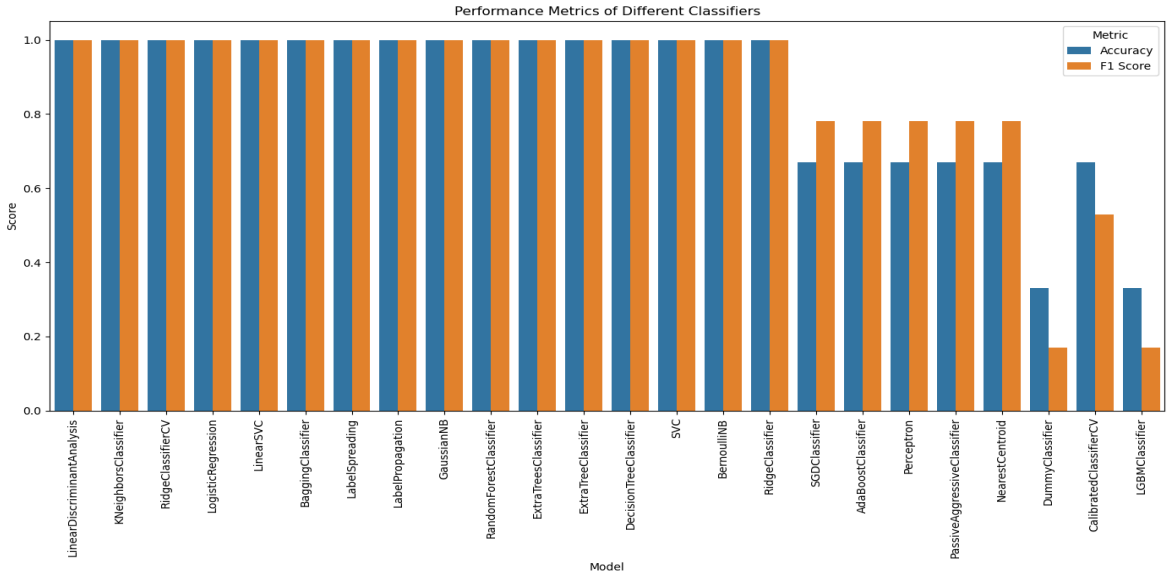


**Figure 5: Lazy Predict results using the CyberVigilance dataset**

**Table 3: Lazy Predict results**

| Algorithm | Accuracy (%) | F1-Score (%) | Time Taken (sec) |
|---|---|---|---|
| **LinearDiscriminantAnalysis** | 100 | 100 | 1.17 |
| **KNeighborsClassifier** | 100 | 100 | 0.02 |
| **RidgeClassifierCV** | 100 | 100 | 0.02 |
| **LogisticRegression** | 100 | 100 | 0.02 |
| **LinearSVC** | 100 | 100 | 0.02 |
| **BaggingClassifier** | 100 | 100 | 0.03 |
| **AdaBoostClassifier** | 67 | 78 | 0.01 |
| **NearestCentroid** | 67 | 78 | 0.01 |
| **LGBMClassifier** | 33 | 17 | 0.52 |

Figure 7 illustrates the predicted outcomes of students' behaviors, with 267 students classified as winners, 191 as losers, and 4 with draws. These results align closely with the student levels, indicating that beginner (losers), intermediate (draw), and expert (winners) players demonstrate distinct performance patterns. Expert students are predominantly predicted as winners, showcasing their stronger grasp of defensive strategies, while beginners are more likely classified as losers, reflecting their developing understanding of cybersecurity tactics. In turn, intermediate players show a more balanced distribution, with occasional draws, highlighting the progression in skills as students advance through the levels (Figure 7). This result can potentially enhance CyberVigilance by tailoring the gaming experience to player skill levels. By categorizing players this way, the game can offer customized challenges and content, ensuring beginners receive appropriate guidance while experts face more advanced tasks.

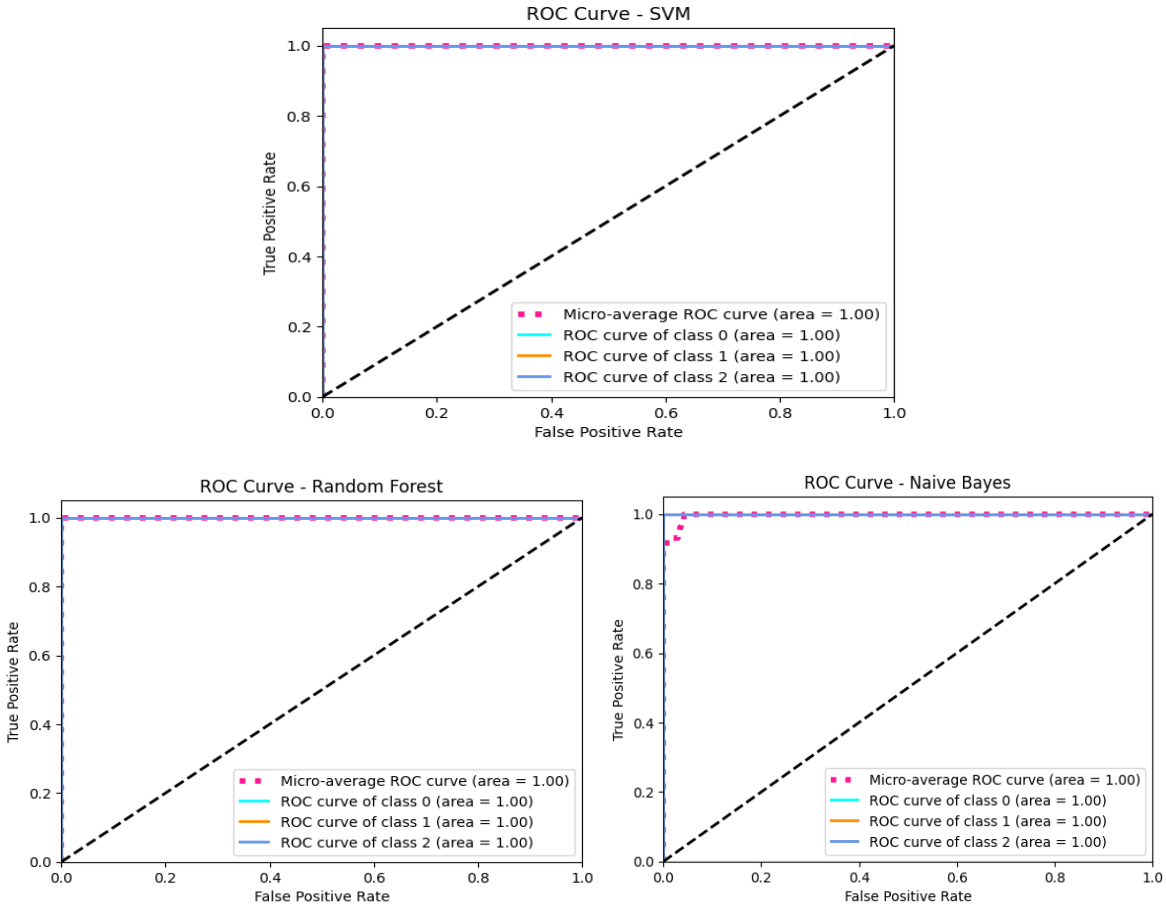


**Figure 6: ML performance using the CyberVigilance dataset**

### 3.1 Discussion

The Random Forest classifier's prediction, showing 267 gameplays won by students, indicates a balanced performance (Figure 7). This result is crucial for ensuring fairness and challenge in gameplay. It suggests that the game mechanics are effectively balanced, with neither side having a significant advantage. This balance is essential for maintaining player engagement and ensuring a competitive and enjoyable experience. While ML models excel in metrics, their feasibility for large-scale data processing or real-time applications must be carefully evaluated (Galván et al. 2011). Additionally, the reliance on these metrics alone does not account for other critical factors such as model interpretability and robustness under different conditions. Nevertheless, capturing and analyzing player performance data to assess the effectiveness of the MAS in predicting and classifying actions using ML directly relates to the research question by providing a way to evaluate how well the CyberVigilance game enhances students' decision-making in cybersecurity. By analyzing gameplay data, ML classifies students' cybersecurity awareness levels, such as expert or beginners (Figure 7), and track improvements over time (Figure 8). The findings indicate that the KNeighborsClassifier, RidgeClassifierCV, LogisticRegression, LinearSVC, and Random Forest models offer both exceptional performance and computational efficiency, making them optimal choices for real-time cybersecurity applications.

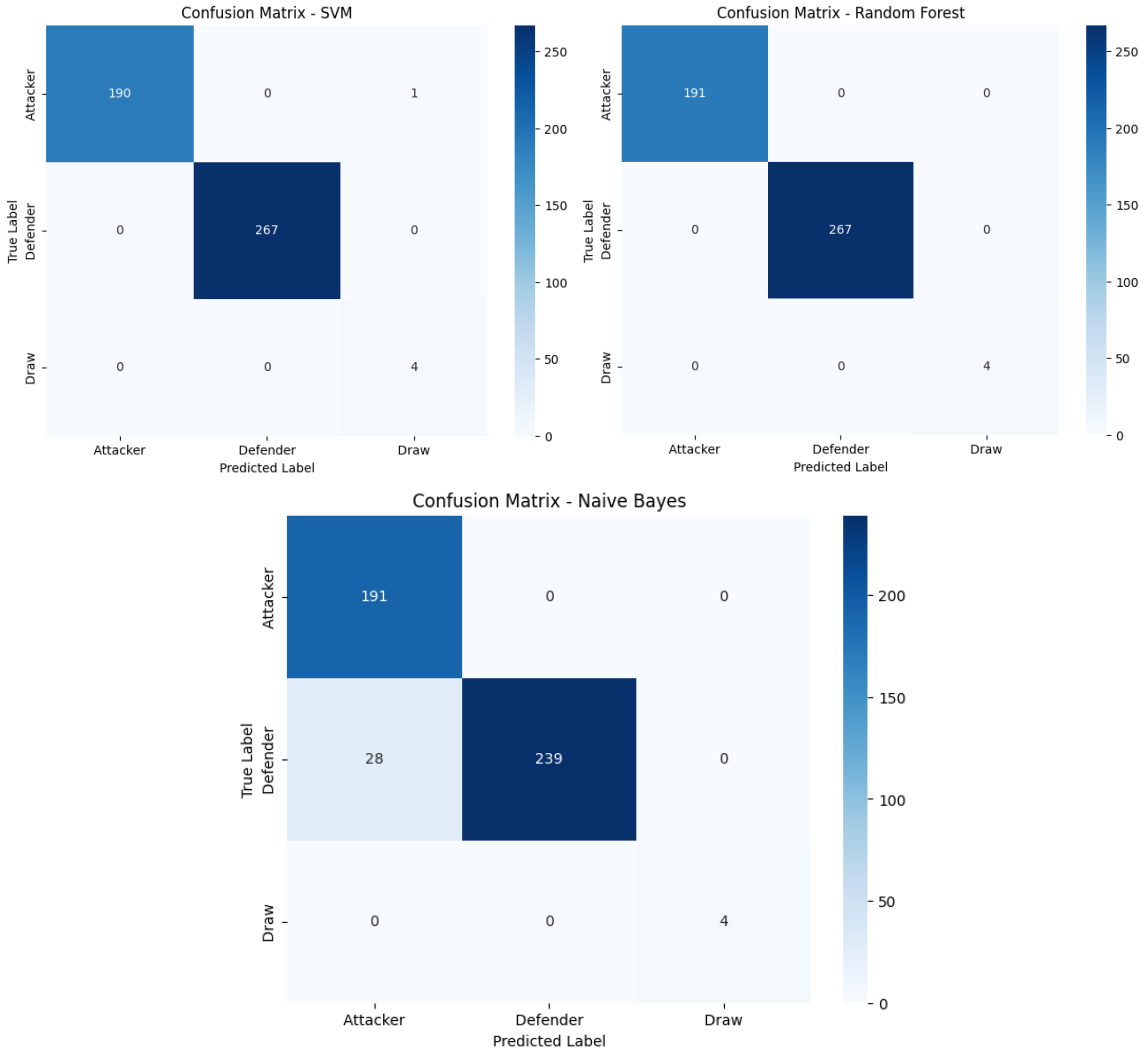


**Figure 7: The confusion matrix's prediction**

These models are highly reliable in predicting and classifying player actions by achieving perfect scores in accuracy, F1-score, and ROC, which is essential in dynamic learning environments like CyberVigilance. Furthermore, their minimal training time enhances their suitability for practical, large-scale use, where swift processing is critical. A thorough analysis of limitations, validity, and threats is essential for a well-rounded understanding of the study's findings. Currently, potential limitations—such as the dependence on simulated game data, which may not fully represent real-world cybersecurity behavior—are not addressed. Additionally, while high-performing models are highlighted, variations in player understanding or engagement levels could impact the accuracy of classification results, posing a threat to external validity.

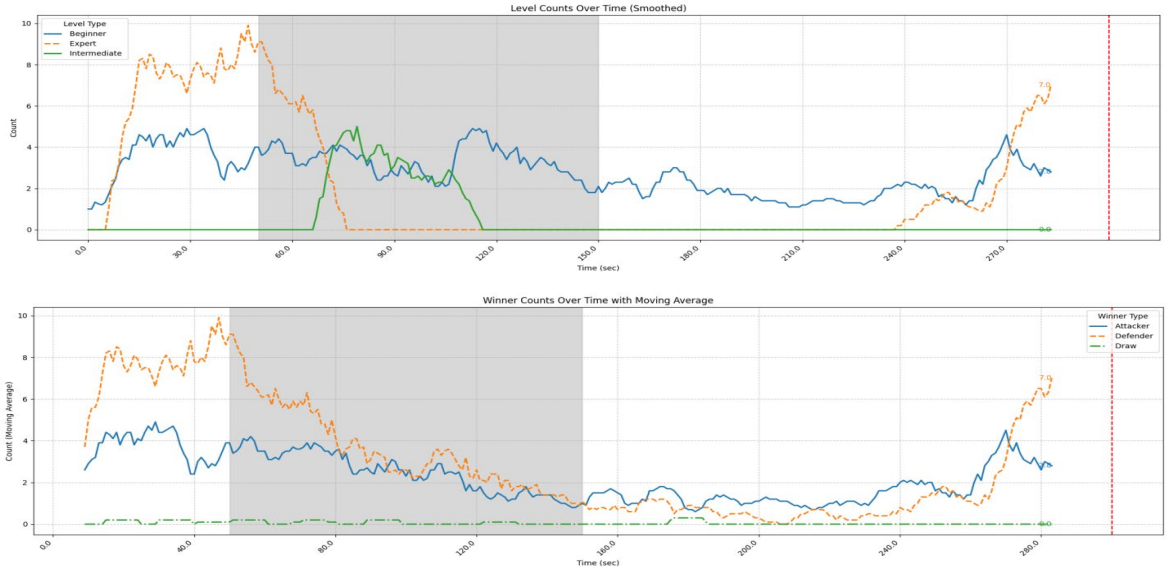


**Figure 8: Students strategy's improvement**

Future work could expand this study by testing CyberVigilance with a larger, more diverse sample of students, including those with varying levels of cybersecurity knowledge, to evaluate how the game adapts across skill levels and demographics. Incorporating real-world cybersecurity incidents into the game scenarios would allow for more complex and realistic decision-making tasks, further enhancing the practical relevance of the training. Developing adaptive ML algorithms that tailor feedback based on individual player performance could increase engagement and effectiveness, offering a personalized learning experience that adjusts in real-time to players' strengths and weaknesses. Lastly, longitudinal studies could be conducted to assess the game's impact on students' long-term cybersecurity skills, providing data on knowledge retention and real-world application post-training.

## 4. Conclusion

This study introduces *CyberVigilance*, an educational, multi-agent cybersecurity game that enhances student decision-making and awareness of cybersecurity principles through interactive, hands-on training. The game's effectiveness is validated through machine learning (ML) analysis, demonstrating that models like KNeighborsClassifier, LogisticRegression, Random Forest, and RidgeClassifierCV provide accurate and efficient classification of player actions. These results confirm that CyberVigilance offers an engaging and effective alternative to traditional cybersecurity education, achieving high accuracy in player classification and potential in predicting learning outcomes. The game's unique feedback and scoring mechanisms foster active learning, enabling students to gain practical experience with defensive strategies against simulated cyber threats. Our findings suggest that integrating ML into game-based training provides actionable insights into player behavior, which could refine and tailor cybersecurity education. Future research will expand the scope of CyberVigilance, testing it on larger and more diverse cohorts and incorporating real-world incident data for increased complexity and relevance. This approach is positioned to offer a scalable, adaptive, and effective tool for cultivating a cybersecurity-ready workforce, addressing a pressing need in the evolving digital landscape.

## References

Asselman, A., Nasseh, A. & Aammou, S. 2018. Revealing strengths, weaknesses and prospects of intelligent collaborative e-learning systems. Advances in Science, Technology and Engineering Systems Journal, 3, 67-79. DOI: 10.25046/aj030310

Bothos, J. M. & Vlachos, V. 2024. Cybersecurity Vulnerability and Risk of Industrial Control Systems. Hybrid Threats, Cyberterrorism and Cyberwarfare. CRC Press.

Chowdhury, N., Katsikas, S. & Gkioulos, V. 2022. Modeling effective cybersecurity training frameworks: A Delphi method-based study. Computers & Security, 113, 102551. https://doi.org/10.1016/j.cose.2021.102551

Eltahir, M. & Ahmed, O. 2023. Cybersecurity awareness in African higher education institutions: a case study of Sudan. Inf. Sci. Lett, 12, 171-183. Doi:10.18576/isl/120113

Fagbule, O. 2023. Cyber Security Training in Small to Medium-sized Enterprises (SMEs): Exploring Organisation Culture and Employee Training Needs. Bournemouth University.

Galván, I.M., Valls, J.M., García, M. and Isasi, P., 2011. A lazy learning approach for building classification models. International journal of intelligent systems, 26(8), pp.773-786. https://doi.org/10.1002/int.20493

Gemade, M.-T. 2022. Using Serious Games designed through the Game ELC+ framework to enhance deep learning in human resources development. University of Westminster.

Gil Ruiz, P. 2024. Gamification as a methodology to enhance analytical and sustainable engagement on social media. Discover Education, 3, 4.

Grobler, M., Gaire, R. & Nepal, S. 2021. User, usage and usability: Redefining human-centric cyber security. Frontiers in Big Data, 4, 583723. Doi:10.3389/fdata.2021.583723

Hassan, J., Devi, A. & Ray, B. 2022. Virtual laboratories in tertiary education: Case study analysis by learning theories. Education Sciences, 12, 554. https://doi.org/10.3390/educsci12080554

Henrio, L., Kammüller, F. & Lutz, B. 2012. ASPfun: A typed functional active object calculus. Science of Computer Programming, 77, 823-847. https://doi.org/10.1016/j.scico.2010.12.008

Jerry-Egemba, N. 2024. Safe and sound: Strengthening cybersecurity in healthcare through robust staff educational programs. Healthcare Management Forum, SAGE Publications Sage CA: Los Angeles, CA, 21-25. https://doi.org/10.1177/08404704231194577

Mukherjee, M., Le, N. T., Chow, Y.-W. & Susilo, W. 2024. Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. Information, 15, 117. https://doi.org/10.3390/info15020117

Nkongolo, M. W. 2024. Infusing Morabaraba game design to develop a cybersecurity awareness game (CyberMoraba). International Conference on Cyber Warfare and Security, 19(1), 240-250. DOI: https://doi.org/10.34190/iccws.19.1.1957

Nkongolo, M. 2023. Game Theory based Artificial Player for Morabaraba Game. 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), IEEE, 1210-1218. Doi: 10.1109/ICSSIT55814.2023.10060972

Nkongolo, M., Tokmak, M. 2023. Zero-Day Threats Detection for Critical Infrastructures. In: Gerber, A., Coetzee, M. (eds) South African Institute of Computer Scientists and Information Technologists. SAICSIT 2023. Springer, Cham. https://doi.org/10.1007/978-3-031-39652-6_3

Oltramari, A., Cranor, L. F., Walls, R. J. & Mcdaniel, P. D. 2014. Building an Ontology of Cyber Security. STIDS, Citeseer, 54-61.

Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I. & Beloev, I. 2024. A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access. DOI: 10.1109/ACCESS.2024.3355547

Pérez-Jorge, D., Martínez-Murciano, M. C., Contreras-Madrid, A. I. & Alonso-Rodríguez, I. 2024. The Relationship between Gamified Physical Exercise and Mental Health in Adolescence: An Example of Open Innovation in Gamified Learning. Healthcare, MDPI, 124. https://doi.org/10.3390/healthcare12020124

Scholefield, S. & Shepherd, L. A. 2019. Gamification techniques for raising cyber security awareness. HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Springer, 191-203.https://doi.org/10.1007/978-3-030-22351-9_13

Stojkovski, B. 2022. User Experience Design for Cybersecurity & Privacy: Addressing User Misperceptions of System Security and Privacy. PhD thesis. University of Luxembourg, Luxembourg City, Luxembourg. Available at: http://orbilu.uni.lu/handle/10993/50982

Sungkur, R. K. 2020. Bridging the training needs of cybersecurity professionals in Mauritius through the use of smart learning environments. PhD thesis. University of Kwazulu Natal.

Tolks, D., Schmidt, J. J. & Kuhn, S. 2024. The Role of AI in Serious Games and Gamification for Health: Scoping Review. JMIR Serious Games, 12, e48258. Doi: 10.2196/48258