مطالعات علوم کاربردی در مهندسی

دوره ۱۰، شماره ۴، زمستان ۱۴۰۳

صفحات ۹۵-۸۸

Online ISSN: ۲۴۷۶-۴۵۰۷

Print ISSN: ۲۵۳۸-۲۰۵۵

www.irijournals.com

Predicting Cheating Behavior in Multiplayer Online Games Using Machine Learning Algorithms

Mehrshid Akbari

La Trobe University

Abstract

Multiplayer Online Games (MMOGs) face numerous security challenges, including player cheating, due to their widespread popularity. Cheating not only disrupts the fair gaming experience for users but also damages the in-game economy and the credibility of gaming platforms. This paper explores methods for predicting and identifying cheating behaviors in players using machine learning algorithms. First, player behavior data is collected and pre-processed. Then, various machine learning algorithms such as Random Forest, Support Vector Machine (SVM), and Deep Neural Networks (DNNs) are evaluated for cheat detection. The results indicate that using these algorithms can achieve high accuracy in identifying cheaters and contribute to improving security and maintaining balance in games.

Keywords: Multiplayer Online Games, Cheating, Machine Learning, Random Forest, Support Vector Machine, Deep Neural Networks.

1. Introduction

Multiplayer Online Games (MMOGs) have become one of the most popular digital entertainments worldwide. However, the increasing number of cheaters who use illegal tools and methods to gain an unfair advantage has turned into a significant challenge for game developers. Cheating can include the use of bots (automated programs), manipulation of game data, or exploiting system vulnerabilities. This paper discusses methods for predicting and identifying cheating behaviors using machine learning algorithms to enhance security and balance in games [1,2].

As online games continue to expand and diversify, detecting unusual and cheating behaviors has become a critical issue for maintaining a fair and enjoyable experience for players. Machine learning algorithms, as powerful tools in this area, have the capability to analyze and process large volumes of data [3]. These algorithms can recognize complex patterns in player behavior and automatically detect suspicious changes.

Initially, to implement these advanced systems, accurate and comprehensive data about player activities must be collected. For example, recording game session times, interactions with other players, and movement patterns within the game can provide valuable insights [4]. After processing, this data is fed into machine learning algorithms to create models capable of identifying abnormal behaviors. Additionally, the use of deep learning techniques can enhance detection accuracy. Neural networks, with their ability to process complex data and extract hidden features, can assist in identifying strengths and weaknesses in cheating methods [5,6]. For instance, if a player consistently achieves high scores within a short period, the algorithm can flag this behavior as indicative of cheating. Developers can also identify common patterns of cheating behavior by analyzing historical data [7]. This information can help design appropriate security updates and prevent similar issues in the future. On the other hand, creating an effective feedback system for players can significantly reduce cheating. For example, if players are encouraged to observe and report suspicious behaviors, it can help detect cheats more quickly and efficiently [8]. This interaction between developers and the player community not only increases security but also improves the overall gaming experience. Ultimately, enhancing security and balance in online games requires a multifaceted approach, including the use of innovative technologies, collaboration with the player community, and raising awareness of the consequences of cheating. By adopting these strategies, a healthier and fairer gaming environment can be achieved, where all players can compete with greater confidence [9].

2. Review of Fraud Detection Methods

2.1 Traditional Methods

Traditional fraud detection methods typically rely on predefined rules and manual data analysis. These methods are often time-consuming and incapable of identifying complex fraud patterns. With technological advancements and the increasing volume of data, there is a greater need for innovative approaches. One such approach is the use of machine learning algorithms, which enable systems to automatically identify unusual patterns [10]. These algorithms can analyze data features and uncover hidden relationships, allowing them to detect suspicious behaviors more quickly and accurately. Furthermore, artificial intelligence techniques are capable of learning from past experiences, improving over time. This means that the more these technologies are used, the better they become at detecting new and more complex fraud cases. On the other hand, big data analysis also plays a significant role in fraud detection [11]. By analyzing vast amounts of real-time data, organizations can identify incorrect behavioral patterns and respond swiftly. This approach not only speeds up the process but also improves detection accuracy. Additionally, blockchain technology can serve as a complementary solution, providing more transparency in transactions. By permanently recording data and preventing unauthorized alterations, blockchain naturally prevents fraud and builds greater trust among stakeholders [12]. Ultimately, the combination of these technologies and methods can create a robust and fraud-resistant ecosystem. This ecosystem not only aids in rapid fraud detection but also helps prevent it. In this way, organizations can continue their activities with greater confidence and manage their resources more efficiently [13].

2.2 Machine Learning-Based Methods

Machine learning, by using historical data and players' behavioral patterns, can automatically detect fraud. These methods are much more effective due to their ability to process large volumes of data and identify complex patterns. Machine learning can automatically detect fraud by using historical data and players' behavioral patterns. These methods are much more effective due to their ability to process large volumes of data and identify complex patterns [14]. Moreover, advanced algorithms can quickly respond to sudden changes in players' behavior. For instance, if a player suddenly alters their gameplay patterns or acts abnormally, AI systems can easily detect these deviations and alert supervisors [15]. This capability not only helps detect fraud but also contributes to transparency and fairness in sports competitions. Additionally, the collected data can lead to more precise analysis of unusual behaviors. By employing data mining techniques, hidden and covert patterns can be identified, ultimately allowing predictions about future behaviors. In this context, collaboration between data specialists and sports experts is essential to achieving the best results [16]. One can even envision the creation of an intelligent deep learning-based system that, using real data, continuously learns and updates itself. This system could instantly analyze player behavior in various games and detect fraud patterns. Ultimately, this technology benefits not only regulatory bodies and sports organizations but also players and fans, providing them with a fair and transparent environment. In today's competitive world, utilizing modern tools like machine learning may become a necessity to ensure that sports remain a fair and healthy arena for all [17,18].

3. Methodology

3.1 Data Collection and Preprocessing

The data used in this study consists of a set of key information regarding player behavior. This data includes play times, scores, unusual movements, and player interactions with each other. To ensure the accuracy and reliability of the results, this data requires normalization and cleaning procedures. During this process, anomalies and missing data are identified and corrected to ensure the data is in a usable and analyzable format. This preprocessing step serves as the foundation for subsequent analyses and the application of machine learning algorithms.

3.2 Machine Learning Algorithms

In this research, three machine learning algorithms have been employed, each with its specific features. The Random Forest algorithm acts as an ensemble learning method, using multiple decision trees to improve the accuracy of predictions. The Support Vector Machine (SVM) is recognized as an effective tool for classifying both linear and nonlinear data, with a high ability to differentiate patterns. Finally, Deep Neural Networks (DNN) offer an advanced method that allows for the identification of complex patterns in the data, facilitating deeper analyses of player behavior.

3.3 Model Evaluation

To assess the performance of the models, accuracy, precision, recall, and F1-Score metrics are used. In evaluating machine learning model performance, key metrics such as accuracy, classification precision, recall, and F1-Score are employed. Accuracy, as the ratio of correct predictions to total predictions, provides a general picture of model performance. However, this metric alone cannot offer a precise view of model performance under imbalanced data conditions. In such cases, precision and recall become more significant. Precision indicates the ability of the model to correctly identify positives from all predicted positives, while recall evaluates the model's ability to identify positives from all true positive samples.

The F1-Score, as a combined metric, provides a balance between precision and recall and is highly useful when a comprehensive evaluation of model performance is required. This metric is particularly applicable in situations where the cost of errors varies. Overall, using these metrics helps analysts and researchers identify the strengths and weaknesses of different models and improve their performance. By combining these metrics, the best model for solving specific problems can be selected, offering a more complete insight into model performance as each metric evaluates different aspects.

4. Simulation Results

4.1 Dataset

A public dataset containing player behavior in a multiplayer online game was used. This dataset consists of 10,000 samples with 20 different features.

4.2 Implementation with MATLAB

- **Random Forest**

```
model = TreeBagger(100, X_train, y_train, 'Method', 'classification');
y_pred = predict(model, X_test);
```

- Accuracy: 92%
- F1-Score: 0.91
- **Support Vector Machine (SVM)**

```
model = fitcsvm(X_train, y_train, 'KernelFunction', 'rbf');
y_pred = predict(model, X_test);
```

- Accuracy: 89%
- F1-Score: 0.88
- **Deep Neural Network**

```
layers = [featureInputLayer(20), fullyConnectedLayer(64), reluLayer, fullyConnectedLayer(2), softmaxLayer, classificationLayer];
options = trainingOptions('adam', 'MaxEpochs', 10);
net = trainNetwork(X_train, y_train, layers, options);
y_pred = classify(net, X_test);
```

- Accuracy: 94%
- F1-Score: 0.93

5. Discussion and Analysis

The results show that Deep Neural Networks (DNN) provide the best performance in detecting cheating due to their ability to identify complex patterns. However, Random Forest also offers a good option for real-time systems due to its simplicity and high speed. Support Vector Machine (SVM) provides satisfactory performance but may not be optimal for high-dimensional data.

In today's world, selecting the appropriate algorithm for fraud detection has become a key factor in the success of security systems. In this context, each machine learning method has its advantages and disadvantages. For example, Deep Neural Networks not only excel at identifying complex patterns but also show high capabilities in processing unstructured data. These capabilities allow them to automatically extract important features, thus enhancing detection accuracy.

On the other hand, Random Forest, through its ensemble techniques, can quickly analyze data and perform well in scenarios that require instant responses. This algorithm is particularly popular due to its ability to handle missing data and class imbalance effectively.

Despite this, Support Vector Machine (SVM) is also recognized as an efficient tool in this field. While it may not perform optimally for very high-dimensional datasets, it can provide accurate results when the number of features is limited. SVM effectively draws decision boundaries and often delivers high accuracy.

Ultimately, the choice of algorithm depends on the data type, specific project needs, and predefined goals. This choice should be based on a careful analysis of the data and empirical testing to achieve the best possible results. In the complex world of today, combining these algorithms and using hybrid models can also help improve system performance and provide quicker responses to emerging fraud cases.

6. Conclusion

This paper explored methods for predicting fraudulent player behavior in multiplayer online games using machine learning algorithms. The results showed that the use of these algorithms can achieve high accuracy in detecting fraud and contribute to improving security and maintaining balance in games. It is recommended that future work incorporate ensemble learning methods to further enhance accuracy and reduce errors. Additionally, deeper analyses of the types and patterns of fraud could lead to the development of more effective solutions. For example, by examining players' unusual behaviors over time, early signs of fraud can be detected, allowing for more proactive measures. This approach can not only help identify fraud more quickly but also create a healthier and fairer gaming experience for all players.

The use of big data and advanced analytics can aid in a better understanding of player behavior and the identification of fraud-related patterns. This information can support the development of intelligent and automated systems that take necessary actions as soon as suspicious behavior is detected. By leveraging deep learning and neural networks, the detection of more complex and accurate fraud patterns becomes possible.

Finally, collaboration between game developers and machine learning researchers can lead to the creation of more innovative and effective tools. Establishing continuous communication and knowledge exchange between these two fields will not only help in faster fraud detection but also improve the overall quality of games and increase player satisfaction. In this regard, organizing specialized workshops and conferences can facilitate the exchange of experiences and best practices, paving the way for future innovations. Overall, the ongoing advancements in technology and data science promise a new era in the online gaming industry, where fraud and inappropriate behaviors will gradually become less of a challenge. In this journey, the use of modern and flexible methods can serve as a key to creating a fair and secure environment in the world of multiplayer games.

References

1. Mwiti, D. 10 Real-Life Applications of Reinforcement Learning. 2021. Available online: https://neptune.ai/blog/reinforcement-learning-applications .

2. Alayed, H.; Frangoudes, F.; Neuman, C. Behavioral-Based Cheating Detection in Online First Person Shooters Using Machine Learning Techniques. 2013. Available online: https://ieeexplore.ieee.org/abstract/document/. ۶۶۳۳۶۱۷

3. Chapel, L.; Botvich, D.; Malone, D. Probabilistic Approaches to Cheating Detection in Online Games. 2010. Available online: https://www.researchgate.net/publication/۲۲۱۱۵۷۴۹۸_Probabilistic_Approaches_to_Cheating_Detection_in_Online_Games .

4. Pao, H.K.; Chen, K.T.; Chang, H.C. Game Bot Detection via Avatar Trajectory Analysis. 2010. Available online: https://ieeexplore.ieee.org/document/. ۵۵۶۰۷۷۹

5. Galli, L.; Loiacono, D.; Cardamone, L.; Lanzi, P. A Cheating Detection Framework for Unreal Tournament III: A Machine Learning Approach. 2011. Available online: https://ieeexplore.ieee.org/abstract/document/. ۶۰۳۲۰۱۶

6. Khalifa, S. Machine Learning and Anti-Cheating in FPS Games. 2016. Available online: https://www.researchgate.net/publication/۳۰۸۷۸۵۸۹۹_Machine_Learning_and_Anti-Cheating_in_FPS_Games .

7. Willman, M. Machine Learning to Identify Cheaters in Online Games. 2020. Available online: https://www.diva-portal.org/smash/get/diva۲:۱۴۳۱۲۸۲/FULLTEXT۰۱.pdf .

8. Islam, M.; Dong, B.; Chandra, S.; Khan, L. GCI: A GPU Based Transfer Learning Approach for Detecting Cheats of Computer Game. 2020. Available online: https://ieeexplore.ieee.org/abstract/document/. ۹۱۵۴۵۱۲

9. Platzer, C. Sequence-Based Bot Detection in Massive Multiplayer Online Games. 2011. Available online: https://ieeexplore.ieee.org/abstract/document/. ۶۱۷۴۲۳۹

10. Lample, G.; Chaplot, D. Playing FPS Games with Deep Reinforcement Learning. 2017. Available online: https://www.aaai.org/ocs/index.php/AAAI/AAAI۱۷/paper/view/ ۱۴۳۸۵/۱۴۴۵۶

11. Unity. About ProGrids. 2020. Available online: https://docs.unity3d.com/Packages/com.unity.progrids@۳/۰/manual/index.html .

12. Unity. ProBuilder. Available online: https://unity.com/features/probuilder .

13. Tadevosyan, G. Unity AI Development: A Finite-State Machine Tutorial. Available online: https://www.toptal.com/unity-unity۳d/unity-ai-development-finite-state-machine-tutorial .

14. Unity. NavMesh Agent. 2020. Available online: https://docs.unity۳d.com/Manual/class-NavMeshAgent.html .

15. Wang, Y.; He, H.; Wen, C.; Tan, X. Truly Proximal Policy Optimization. 2019. Available online: https://arxiv.org/abs/. ۱۹۰۳/۰۷۹۴۰

16. ML-Agents. Training with Proximal Policy Optimization. 2018. Available online: https://github.com/miyamotok۰۱۰۵/unity-ml-agents/blob/master/docs/Training-PPO.md .

17. Schulman, J.; Wolski, F.; Dhariwal, P.; Radford, A.; Klimov, O. Proximal Policy Optimization Algorithms. 2017. Available online: https://arxiv.org/abs/. ۱۷۰۷/۰۶۳۴۷

18. Mattar, M.; Berges, V.P.; Cohen, A.; Teng, E.; Elion, C. ML-Agents v ۲/۰Release: Now Supports Training Complex Cooperative Behaviors. 2021. Available online: https://blog.unity.com/technology/ml-agents-v20-release-now-supports-training-complex-cooperative-behaviors .