zensar

Gaming Platform Enlists AI to **Detect and Neutralize Threats**

Case Study

Overview

Building defenses for an online gaming platform

An online gaming platform, at the forefront of the gaming revolution for over three decades, wanted to address fraudulent activities among players that could harm the platform's reputation and financial stability. The concerning fraudulent behavior included unauthorized transactions, bonus abuse, and suspicious session patterns.

Zensar's brief:
Deploy a solution to identify and prevent fraudulent activities related to utilization of incentives such as free games, bonuses, and random prizes on the gaming platform.

Beyond the brief:
Our comprehensive solution not only addressed existing risks related to fraud, but also laid the foundation for mining valuable insights from new data on emerging fraud patterns — ensuring the integrity and security of the online gaming platform in the future.

An RPG Company

Challenges

Impact to the bottom line and the top line

The client was concerned about the undesirable consequences of fraud in online gaming:

- **Financial losses:** Fraudulent activity in online gaming could result in significant financial losses for both players and the platform.
- **Reputation damage:** Fraudulent activity could damage the reputation of the online gaming platform, leading to a loss of trust and customers.
- **Ineffective detection:** Inefficiency in the current methods of fraud detection could lead to time-consuming and tedious manual reviews of transactions.

Solution

Application for fraud detection

Our goal was to identify patterns for potentially fraudulent activities within online gaming transactions and translate them into robust algorithms for effective fraud prevention. As our client's technology partner, we collaborated with the client's team every step of the way across four phases of solution deployment:

Discovery: We gathered information on wagers, withdrawals, and deposits from the online gaming platform to gain a foundational understanding of financial transactions within the system. In the process, we realized that there was a lack of labeled data, which made it challenging to develop a supervised machine learning (ML) model for fraud detection.

Planning: We mined the data for valuable insights into user behavior, such as bet amounts, bonus event frequency, and deposit variability. This helped us identify potential fraud patterns and understand normal user activity. We then explored an unsupervised algorithm that identifies anomalies in the data without requiring labeled data.

Designing: We adopted an ensemble method that combines anomaly detection with a rule-based system, employing both statistical anomalies and domain-specific knowledge, to enhance fraud detection capabilities. These were the key components of the solution strategy:

- **Rule-based methods:** This involved multiple hypothesis creation, based on context:
  - Bet amount rule: If a user's bet amount is greater than 2x their average bet amount, flag as potential fraud.
  - Deposit amount rule: If a user's deposit amount is greater than 2x their average deposit amount, flag as potential fraud.
  - Withdrawal amount rule: If a user's withdrawal amount is greater than 2x their average withdrawal amount, flag as potential fraud.

- **Isolation forest:** Here, we used artificial intelligence (AI) to identify synthetic identities by analyzing data inconsistencies and differences in behavioral patterns. The highlights:
  - Unsupervised algorithm to identify anomalies in the data without requiring labeled data
  - Combination of decision trees to identify potential fraud patterns

    Fraud score for each transaction based on the user behavior, with higher scores indicating a higher likelihood of fraud

- **Feature engineering:** Our solution relied on four categories of engineered features, each contributing uniquely to fraud detection:
  - Original features directly extracted from the data sources to provide foundational insights into transactions and user behavior
  - Refined features engineered from the original features to capture specific patterns indicative of fraudulent behavior
  - Causal features derived from hypothesized causal relationships between variables to provide additional insights into user behavior
  - Rule-based features where binary flags are triggered by predefined rules, based on domain expertise, to quickly identify known suspicious patterns

Implementation: The trained model performs real-time scoring of user sessions to detect a potential fraud. If a session's “suspiciousness” crosses the threshold score set, the session is classified as a fraudulent one and operators are notified to prevent further suspicious activities. In addition, the performance of the model is continuously monitored to make necessary adjustments and increase the accuracy of fraud detection.

Solution enablers

- **Azure Machine Learning (Azure ML)** was used to train, deploy, and manage ML models at scale and support ensemble solutions combining rule-based methods and AI/ML.

- **Azure Kubernetes Service (AKS)** was used to deploy ML models as web services, host and scale containerized fraud detection models, and support auto-scaling of gaming workloads.

- **Azure Databricks** was used for big data processing, feature engineering, and ML model development, as well as native integration with Azure ML for seamless deployment.

- **Azure Functions** was used to enable serverless computing for real-time, rule-based fraud detection logic and deliver cost-effective event-driven operations.

- **Azure Event Hubs** was used to enable live fraud detection with real-time data streaming and low-latency data ingestion.

- **Azure Logic Apps** was used to automate workflows for fraud detection alerts and actions and simplify integration with external systems.

- **Azure SQL Database and Azure Cosmos DB** were used for efficient storage and retrieval of fraud-related data and leverage high availability and low latency for addressing gaming data queries.

- **Azure Monitor Application Insights** was used to enable end-to-end monitoring of the deployed fraud detection solution by leveraging features for easy integration with Azure ML and AKS.

Impact

Fortified gaming platform

- Prompt detection of suspicious behavior enabled by real-time scoring of user sessions
- Safer experience for legitimate users enabled by effective fraud prevention
- Reduced manual effort and streamlined processes enabled by automated fraud detection

Business outcomes: By detecting and preventing fraudulent activities in real time, the solution has helped improve player experience, ensure fair play, and minimize financial losses due to fraud.

At Zensar, we're 'experience-led everything.' We are committed to conceptualizing, designing, engineering, marketing, and managing digital solutions and experiences for over 145 leading enterprises. Using our 3Es of experience, engineering, and engagement, we harness the power of technology, creativity, and insight to deliver impact.

Part of the $4.8 billion RPG Group, we are headquartered in Pune, India. Our 10,000+ employees work across 30+ locations worldwide, including Milpitas, Seattle, Princeton, Cape Town, London, Zurich, Singapore, and Mexico City.

For more information, please contact: **info@zensar.com | www.zensar.com**