ScamShield - Detecting Suspicious Calls Using AI

Introduction to ScamShield

Exploring the Challenge, Objective and Competitive Edge

Hackathon Challenge

To develop a robust AI-based solution capable of identifying and mitigating suspicious activity in telecommunication, thereby enhancing user safety.

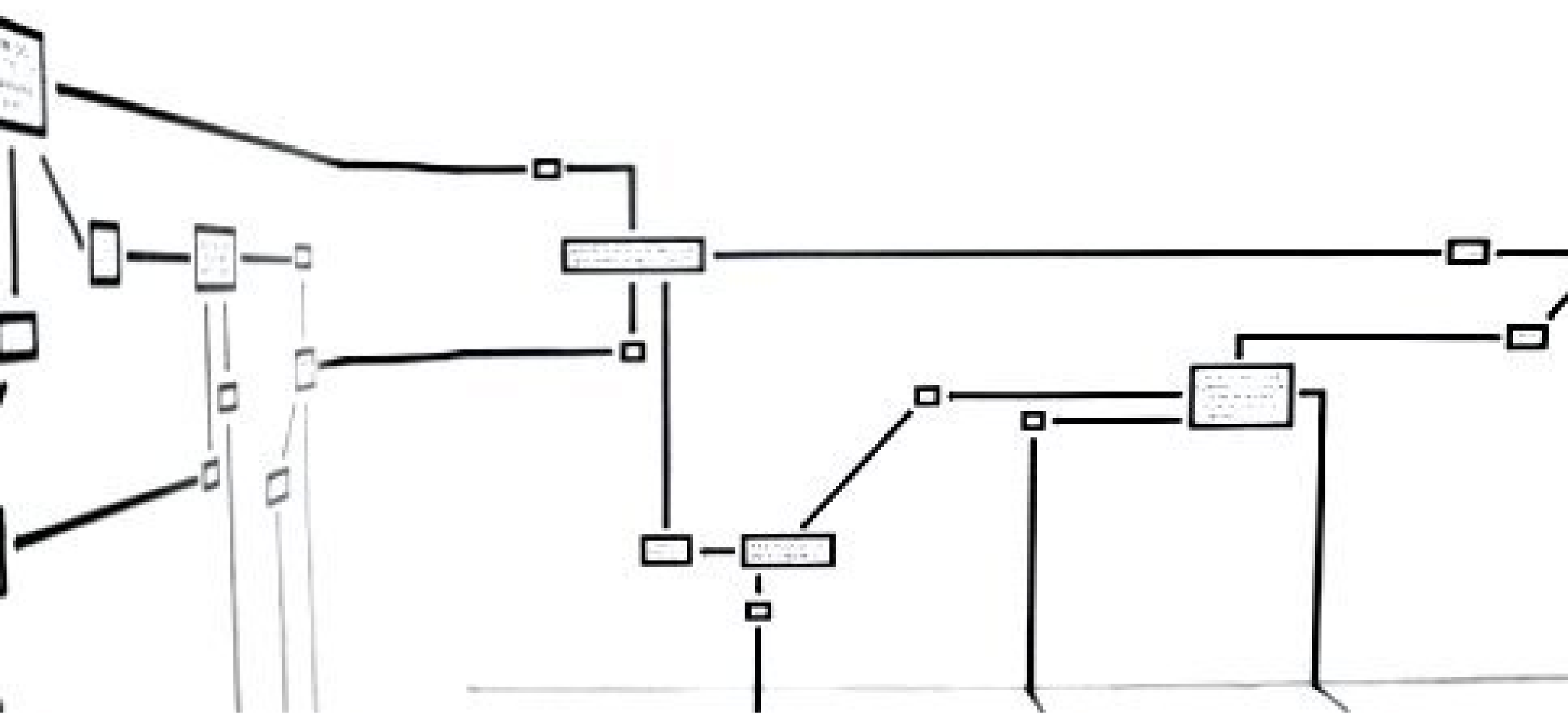
Objective

The primary goal is to design a system that leverages machine learning algorithms to effectively analyze call patterns and detect anomalies indicative of scams.

Competitive Edge

Our approach integrates advanced neural networks and real-time analytics, transforming call detection into a proactive defense mechanism against fraud.


USERS: LAST 7 DAYS USING MEDIAN
LOAD TIME VS BOUNCE RATE
OPTIONS
37.1%
START RENDER VS BOUNCE RATE
OPTIONS
PAGE VIEWS VS ENGAGE
OPTIONS
0.7s
2.7Mpvs
40.6%
SESSIONS
OPTIONS
479K
17min
2pvs



Constraints & Considerations

Navigating Challenges in Development

Accuracy
Maintaining a high level of accuracy in detection is paramount to prevent false positives and ensure user confidence in the system.

Efficiency
The system must process data without significant delays, balancing thorough analysis with swift response times to potential threats.

Innovation
Ongoing innovation is essential to keep the system ahead of evolving scam tactics, necessitating an adaptive algorithm.

Security & Privacy
Data handling needs to adhere to stringent security protocols and regulatory compliance to protect users' sensitive information.

Evaluation Metrics

Assessing Effectiveness of ScamShield

- **Accuracy:** The ability of the system to correctly identify fraudulent calls, minimizing both false negatives and false positives.
- **Explainability:** The degree to which the AI's decision-making process is transparent and understandable to users, facilitating trust and refinement.
- **Efficiency:** Speed of the system in processing input data and producing timely alerts, critical for real-time monitoring applications.
- **Innovation:** Evaluating the uniqueness of the methods employed, including cutting-edge technologies that enhance detection and classification capabilities.
- **Scalability:** The capacity of the system to handle increased loads as user demand grows without compromising performance.

Conclusion & Future Directions

Looking Ahead to Enhanced Fraud Detection

Future of Fraud Detection
nticipating advancements in AI technology will pave the way for more sophisticated fraud detection solutions that adapt to new threats.

User Protection
Ensuring users are safeguarded against rising scam tactics through proactive measures and real-time alerts enabled by AI.

Enhancing Cybersecurity
Integrating our findings into broader cybersecurity frameworks to bolster defenses against complex digital threats.

Revolutionizing Detection
The comprehensive approach signifies a shift towards more effective and proactive systems in identifying and thwarting fraud.