Deep Learning Based Fraudulent Login Detection System

Harshitha H B[1] Abhineeth Aalthoor[2] B R Yashaswini[3] C Smriti Emmanuel[4] Kushal Mandivya[5]
[1,2,3,4,5]Department of Computer Science and Design
[1,2,3,4,5]ATME college of Engineering, Mysuru, India

Abstract — With the rapid evolution of digital technology, securing user accounts has become an increasingly crucial challenge. Traditional authentication mechanisms, including passwords and static rule-based security protocols, have become vulnerable to cyber threats such as credential stuffing, phishing, and brute-force attacks. This paper presents an AI-powered system to enhance login security by analyzing user behavior and detecting anomalous activities indicative of fraudulent logins. By employing a machine learning-based approach, the system evaluates key factors such as IP address, geographical location, login frequency, and device fingerprinting to detect unauthorized access attempts. The model dynamically adapts to new threats by continuously learning from historical login patterns. The proposed solution enhances cybersecurity while maintaining a seamless user experience by minimizing false positives.

Keywords: Anomaly Detection, AI-Based Security, Behavioral Authentication, Fraud Prevention, Machine Learning, Cybersecurity

I. Introduction

With the growing dependency on digital platforms, ensuring robust authentication mechanisms is imperative for protecting sensitive data. Conventional password-based authentication methods often fail due to poor password hygiene, phishing attacks, and large-scale data breaches. Advanced cyber threats such as botnet-driven credential stuffing and social engineering attacks exploit these vulnerabilities, making it difficult to distinguish between genuine and fraudulent login attempts.

To address these concerns, this paper proposes an AI-driven fraudulent login detection system that leverages behavioral analytics and anomaly detection techniques. By monitoring key login parameters such as IP address variations, device type, round-trip time (RTT), and login time, the system can identify deviations from a user's typical login behavior. Upon detecting suspicious activity, the system triggers additional authentication measures or blocks access entirely.

The proposed model ensures an intelligent and adaptive security framework that evolves in response to emerging cyber threats, thereby providing a proactive defense against unauthorized access.

II. Methodology

The system integrates machine learning techniques with behavioral analytics to identify fraudulent login attempts. The key steps in the methodology include data acquisition, preprocessing, model training, and real-time inference.

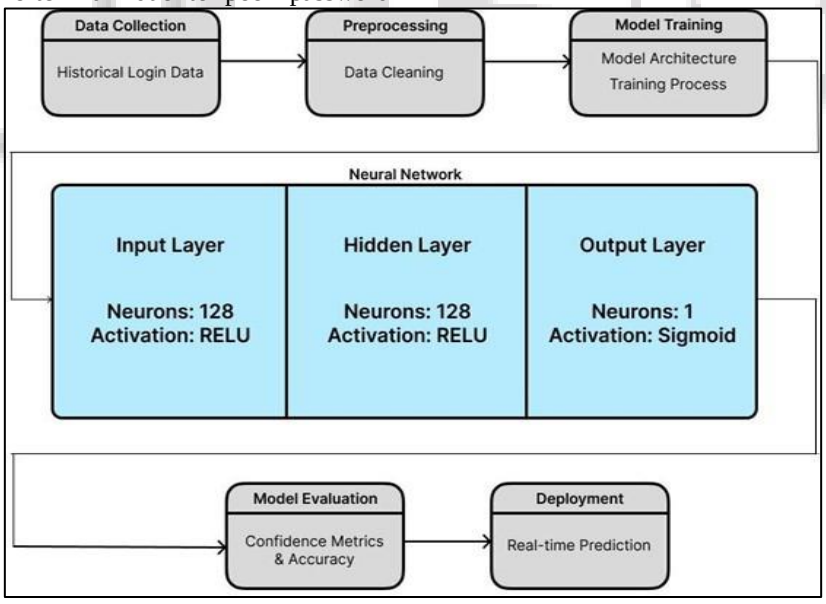

Fig. 1: System Methodology

Step 1: Data Collection and Storage

- The system extracts login data from a relational database, recording attributes such as IP addresses, geolocation, timestamps, device identifiers, and authentication outcomes.
- Data is periodically updated to refine the AI model and improve detection accuracy.

Step 2: Data Preprocessing

- The collected data undergoes preprocessing, including:
  - Noise Reduction: Eliminating incomplete or corrupted entries.
  - Feature Encoding: Converting categorical attributes (e.g., device type, geolocation) into machine-readable formats using one-hot encoding.
  - Normalization: Standardizing numerical attributes such as login time intervals and RTT values to ensure uniformity.

Step 3: Machine Learning Model Development

- A Fully Connected Neural Network (FCNN) is designed using TensorFlow and Keras.
- The architecture comprises:
  - Input Layer: Accepts login attributes as feature vectors.
  - Hidden Layers: Multiple dense layers with ReLU activation for feature extraction.
  - Output Layer: Sigmoid activation function for binary classification (legitimate vs. fraudulent login attempts).
  - The model is trained on historical login data with supervised learning techniques to enhance accuracy.

Step 4: Real-Time Detection & Decision Making

- Upon a new login attempt, the system evaluates the risk score based on previous patterns.
- If the probability of fraudulent behavior exceeds a predefined threshold, additional authentication steps (such as multi-factor authentication) are triggered.
- Suspicious login attempts are flagged, and alerts are generated for further review.

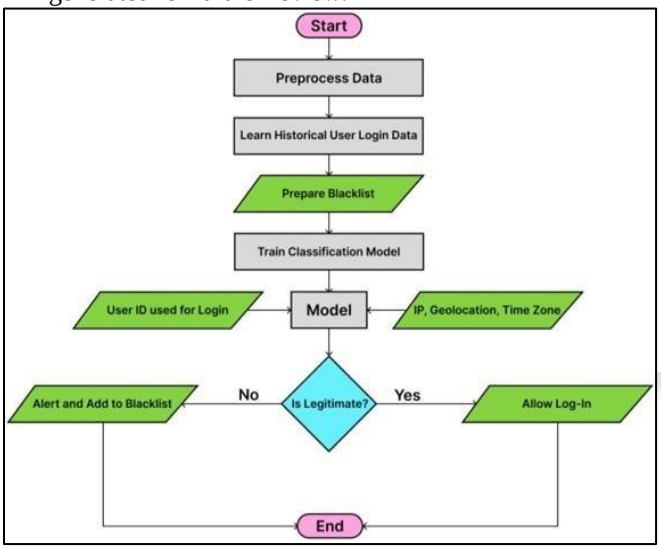

Fig. 2: System Implementation

III. Results

To evaluate the effectiveness of the system, real-time login data was tested against the trained model.

A. Experimental Setup

- Dataset: 10,000 login attempts, including both legitimate and fraudulent attempts.
- Evaluation Metrics: Accuracy, precision, recall, and F1-score.
- Implementation Tools: TensorFlow, Keras, NumPy, Pandas, and SQLite3.

B. Findings

- Detection Accuracy: The model achieved an accuracy of 98.7% in identifying fraudulent logins.
- False Positives & Negatives: Minimal false positives ensured that legitimate users were not unnecessarily blocked, while high recall minimized missed fraud cases.
- Performance Optimization: Feature selection and hyperparameter tuning contributed to improved model efficiency.

These results indicate that AI-based behavioral analysis is an effective approach for detecting fraudulent login attempts in real-time.

IV. Conclusion

This paper presents an AI-driven system for fraudulent login detection, offering an advanced security solution by leveraging machine learning techniques. The system effectively identifies unauthorized login attempts by analyzing behavioral patterns and contextual data, significantly improving cybersecurity in online platforms.

Future work will explore the integration of additional security measures such as biometric authentication, behavioral biometrics, and federated learning for enhanced privacy-preserving fraud detection. Further improvements in model interpretability and adversarial robustness will enhance real-world applicability across various industries, including finance, healthcare, and e-commerce.

References

[1] S. Gupta, R. Rathi, "Role of Artificial Intelligence in Detecting and Preventing Financial Fraud," Journal of Big Data, 2023.
[2] P. Zanke, "AI-Driven Fraud Detection Systems: A Comparative Study across Sectors," IEEE Conference Proceedings, 2023.
[3] H. Shen, E. Kurshan, "Deep Q-Network-Based Adaptive Alert Threshold Selection Policy for Payment Fraud Systems," arXiv, 2020.
[4] N. Yousefi, M. Alaghband, "Machine Learning Techniques for Credit Card Fraud Detection," arXiv, 2019.
[5] M. Ebad, "Fraud Detection in Banking Transactions Using Machine Learning," International Conference on Financial Innovation and Economic Development, 2023.