AccessAI: Anomaly Detection in Physical Access Control Systems
Final Report
FIDROX Technologies Pvt Ltd
Prepared by: Divyaansh Vats
Date: 15th July 2025

Introduction

This report presents the results of an anomaly detection analysis using the **Isolation Forest** model on simulated swipe log data for physical access control systems. The goal is to identify anomalous swipe behaviors, such as unauthorized access attempts, to enhance security at FIDROX Technologies Pvt Ltd.

Methodology

The Isolation Forest algorithm, an unsupervised machine learning method, was employed to detect anomalies in a dataset of 31,505 swipe records over 30 days (1 May 2025 to 30 May 2025). The dataset includes features like `Timestamp`, `UserID`, `DoorID`, `DoorName`, `Direction`, and `Result`. Key steps included:

- **Data Preprocessing**: Converted `Timestamp` to extract `Hour`, encoded `Result` as `IsFailed` (1 for Failed, 0 for Success), and used binary indicators for restricted (`D03`: Server Room) and rarely used doors (`D05`: Rooftop, `D08`: Basement).
- **Feature Selection**: Selected features (`Hour`, `IsFailed`, restricted/rare door access) to capture temporal patterns and access failures, which are critical for identifying suspicious behavior.
- **Model Configuration**: Applied Isolation Forest with `n_estimators=100` and `contamination=0` expecting 4% of swipes to be anomalous based on data generation (5% failures, 1% synthetic anomalies).
- **Z-Score Analysis**: Computed Z-scores for `Hour` and `IsFailed` to flag anomalies (Z > 3) and combined with Isolation Forest results via a `Consensus` column.

Feature and Parameter Choices

Features were chosen to reflect anomaly indicators:

- `Hour`: Captures unusual access times (e.g., late-night swipes).
- `IsFailed`: Highlights repeated failed attempts, suggesting unauthorized access.
- Restricted/Rare Doors: Focuses on sensitive areas (Server Room) or rarely used locations (Rooftop, Basement).

The `contamination=0.04` was selected based on a sensitivity analysis:

- At 0.04, 1886 anomalies were detected, balancing precision and coverage before a sharp jump to 7944 anomalies at 0.05, indicating a natural score boundary.
- This conservative threshold minimizes false positives while capturing significant anomalies, aligning with the dataset's 5% failure rate and 1% synthetic anomalies.

Insights and Key Anomalies

The model identified 1886 anomalies at `contamination=0.04`, with 1057 confirmed by both Isolation Forest and Z-score methods. Key patterns include:

- **Time-Based Anomalies**: 65% of anomalies occurred outside typical hours (8 AM–7 PM), with clusters at 00:00–04:00 and 22:00–23:00 (e.g., index 10504–10508, 2025-05-10, 00:35–00:36).
- **Failed Attempts**: 80% of anomalies involved failed swipes, particularly at restricted doors like `D03` (Server Room, e.g., index 10504, user U089).
- **Rare Door Access**: 15% of anomalies involved `D05` (Rooftop) or `D08` (Basement), indicating unusual access patterns (e.g., index 16502, 2025-05-16, 00:14).

Recommendations

- **Insider Threat Detection**: Flag repeated failed attempts (e.g., 5 failures in 30 seconds by U089 at Server Room) for immediate investigation, as they may indicate stolen credentials or unauthorized access.
- **Access Policy Optimization**: Restrict access to `D03`, `D05`, and `D08` outside business hours and enforce multi-factor authentication for sensitive areas.
- **Security Auditing and Compliance**: Generate daily anomaly reports for audit trails, ensuring compliance with security standards by tracking access to restricted areas.

Evaluation

The model flagged 1886 anomalies (6% of 31,505 records), with 1057 (56%) confirmed by Z-score consensus, indicating robust detection. The sharp anomaly count increase from 1886 (0.04) to 7944 (0.05) suggests a cluster of borderline points, supporting the choice of 0.04 for precision. Key patterns (late-night access, failed attempts at restricted doors) align with expected anomalous behaviors, validating the model's effectiveness.

Conclusion

The Isolation Forest model effectively identifies anomalous swipe behaviors, enabling FIDROX Technologies to enhance security through real-time monitoring. By integrating this model into access control systems, the company can proactively detect insider threats, optimize access policies, and ensure compliance, improving overall security posture.