PSB's FinTech Cybersecurity Hackathon 2025 Solution Approach

Project Name: FraudShield+
Problem Statement:
Impersonated Registration/Frauds in Mobile & Internet Banking along with behavior based user authentication with password less login

Team Name: TEAM ARJUNA

Date: July 29, 2025

Summary:

An advanced fraud detection system called FraudShield+ was created to protect online and mobile banking while users are registering and logging in. It incorporates behavioral biometrics, FIDO2 password-less authentication, and ongoing SIM, device, and geolocation data monitoring. This multi-layered strategy guarantees that fraudulent access is prevented even in the event that attackers have legitimate credentials or OTPs. Improved customer trust, fewer account takeovers, and real-time fraud monitoring via admin dashboards are all advantageous to financial institutions.

The Problem Statement:

In order to obtain unauthorized access to banking accounts, sophisticated fraudsters are increasingly employing strategies like device spoofing, phishing, and SIM swaps. For banks and their clients, this results in serious financial and reputational harm.

- **Issue:** Accounts are susceptible to fraudulent new device registrations and takeovers because standard security measures, such as OTPs, are susceptible to interception.
- **Impact:** High operating expenses for fraud investigation, deterioration of consumer trust in digital banking platforms, and monetary losses for consumers.
- **Target User:** Bank customers using mobile/internet banking and the bank's fraud analysis team.

Our Proposed Solution:

FraudShield+ is a complete security engine that creates a strong, intelligent defense layer by integrating with current banking platforms. It functions by:

- **Core Functionality 1:** Real-Time Risk Scoring: To produce a real-time risk score, each login or registration attempt is compared to a profile of the user's usual device, SIM, location, and behavior.

- **Core Functionality 2:** Adaptive Authentication: depending on the risk score, the system instantly blocks high-risk attempts, automatically authorizes low-risk requests, and challenges medium-risk ones with additional verification (such as biometrics).
- **Core Functionality 3:** Admin Intelligence Dashboard: This tool helps bank administrators proactively manage threats by giving them a real-time view of alerts, risk trends, and location mismatch maps.

Data Sets to be Used:

Since actual banking data is private, realistic, artificially generated datasets are used to develop and illustrate our model.

Data Set Name	Source	Description	Intended use in Solution
Users & Devices	Generated using Faker/ Synthetically Generated	Includes information about trusted devices (DeviceID, OS, device type), as well as user profiles with contact details (UserID).	To create a reference point for the appearance of a typical user's devices
Login History	Generated using synthetic data	A set of login attempts that include device IDs, timestamps, IP addresses, and geolocation (latitude/ longitude)	To spot anomalies in login patterns, like odd times or places.
SIM Profile	Created synthetically	Provides a phone number along with details about the SIM card ID and the date of the most recent SIM swap.	To report recent SIM swaps, as these are important signs of fraud.
Behavioral Profile	Generated using synthetic data	Monitors user activity, including mouse movements, typing speed, and screen interaction patterns.	To identify attempts at impersonation by looking for behavioral abnormalities.
Threat Intelligence	Synthetically generated	A list of blacklisted device fingerprints, phishing websites, and known malicious IP addresses.	To compare login attempts to malicious patterns and known security threats.

Solution Approach & Technical Architecture

- **Technical Stack:**

•**Backend:** Python (Flask)

•**AI / Machine Learning:** Scikit-learn, TensorFlow, Pandas

•**Database:** PostgreSQL, MongoDB

•**Geolocation & Notifications:** Geopy, IPStack API, Twilio (SMS), Firebase (Push), Gmail SMTP (Email)

•**Authentication:** FIDO2 / WebAuthn(Web Authentication API)

•**Dashboard:** Streamlit / Dash

•**Deployment:** Docker, AWS EC2

- **System Architecture & Data Flow**

User Attempt: A user registers a new device or logs in.

Data Collection: The device fingerprint, IP address, and behavioral patterns (like typing speed) are all transparently gathered by the system.

Extraction of Features: In order to determine

- whether this is a new device, the backend queries its database.
- Has there been a recent SIM swap (less than 72 hours ago)?
- Does the location (e.g., > 300km) differ from previous logins?
- Is there a difference between the user's behavior and their profile?

Risk Scoring: Using these characteristics, the Risk Scoring Engine determines a weighted score.

Choice & Action:

- Low Risk (<30): Give the transaction approval.
- Medium Risk (30–60): Difficulty using FIDO2 biometrics or an additional step-up authentication method.
- High Risk (>60): Block transactions and notify the user and bank administrator right away.

Dashboard Update: The admin dashboard displays and logs the event and its result.

- **Fundamental Model/Algorithm**

A weighted, rule-based Risk Scoring Engine forms its core. It uses definite, highly significant indicators to assign risk.

Key attributes and weights:

- New SIM swap (less than 72 hours ago): +40 points
- Untrusted/New Device: +30 points
- Considerable Location Inconsistency (>300 km): +20 points
- Anomalies in behavior (such as a typing speed deviation of more than 20%): +20 points
- +10 points for the Threat Intelligence Match

- **The component of machine learning:** An important input feature for the primary scoring engine is the detection of anomalies in behavioral biometrics using a TensorFlow/Scikit-learn model.

Innovation & Unique Value Proposition (UVP)

- **Multi-Layered Defense:** Combines device, SIM, location, and behavioral analysis to go beyond single-factor checks (like OTP).
- **Inclusivity by Design:** Makes sure no customer is left behind by supporting both older keypad phones (with IVR/SMS alerts) and contemporary smartphones (with FIDO2).
- **Proactive, not reactive:** identifies and stops fraud before it occurs rather than after it has happened.
- **Privacy-Compliant:** Alerts are made to provide information without disclosing private information.

Conclusion:

In summary, our concept offers a cutting-edge, multi-layered fraud detection platform capable of addressing contemporary threats in the banking sector. With capabilities such as behavioral biometrics, SIM and device profiling, and cloud-native scalability, it provides a solid foundation for secure real-world deployment. Our concept is not only technically robust but also flexible and future-proof—positioning it with high potential for growth and real-world application.