



IOB CYBERNOVA HACKATHON 2025

AI POWERED SECURE AUTHENTICATION SYSTEM



Problem Statement Title-To enhance the security of banking system and provide a seamless user experience

Theme- AI Powered Security System

PS Category- Software

Team ID- 8

Team Name : Exception Handlers

Team Members :	RRN & Dept
Syed Tufail Ahmed	220191601058-B.Tech CSE(IOT)
Sabeer Sulaiman Khan	220191601053-B.Tech CSE(IOT)
Syed Shabib Ahmed	220171601124-B.Tech AI&DS-B
Syed Mustafa	220171601123-B.Tech AI&DS-B



PROBLEM STATEMENT

- 1.Reduce Password Dependency.
- 2.Lack of Real Time Monitoring.
- 3.SMS OTP Weaknesses.
- 4.Inadequate Phishing Defense.



"67% of consumers reuse banking passwords on other sites, making them vulnerable."

-Federal Reserve Bank



"Lack of Real Time User Monitoring in Banks can lead as much 40% losses."

-McKinsey & Company



"Chase Bank (2020) – Attackers bypassed SMS OTPs via SIM swaps, stealing \$600K+ from accounts."

-Chase Bank

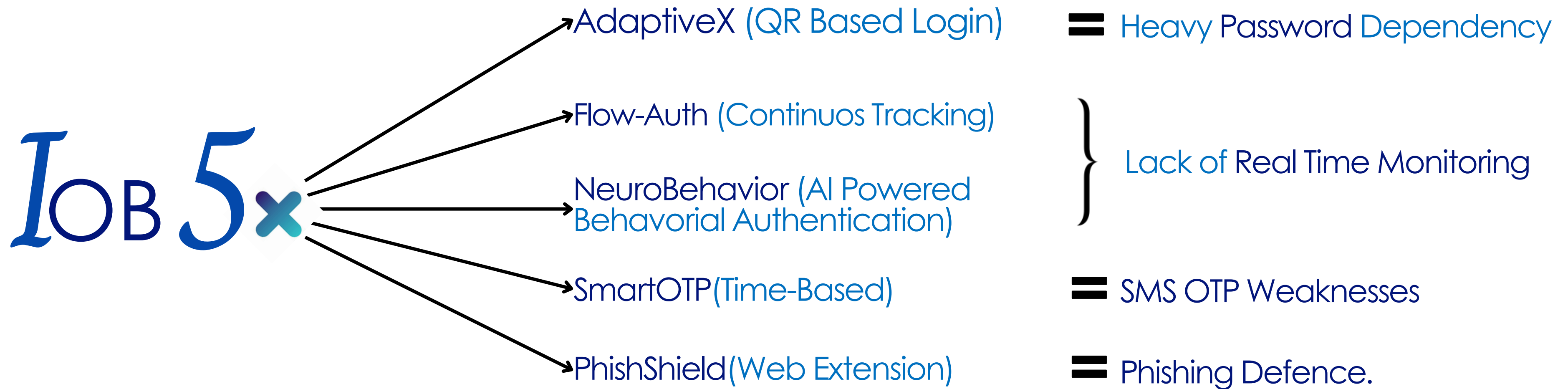


"Fraudsters cloned HSBC's website, stealing credentials from 10,000+ users."

-HSBC Bank

PROPOSED SOLUTION

IOB 5x is a **Five-in-One Solution** that the Team Exception Handlers Have come up with to solve the said problems in current banking systems.

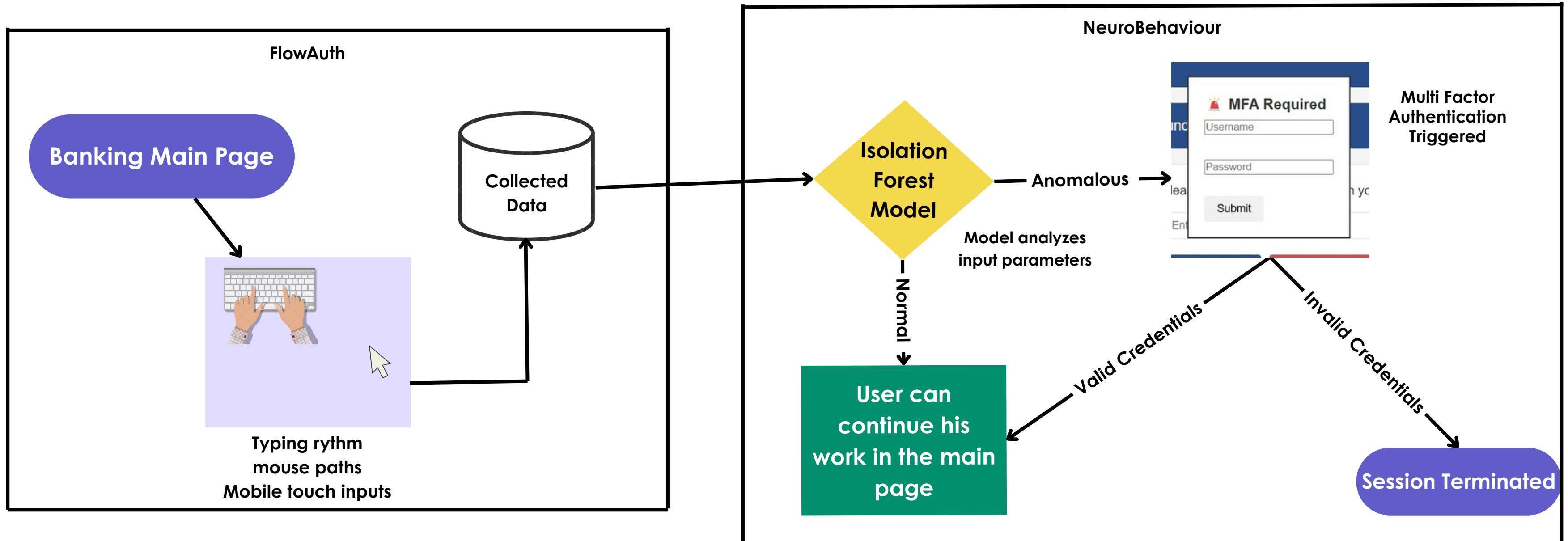


1) AdaptiveX (QR Based Login)



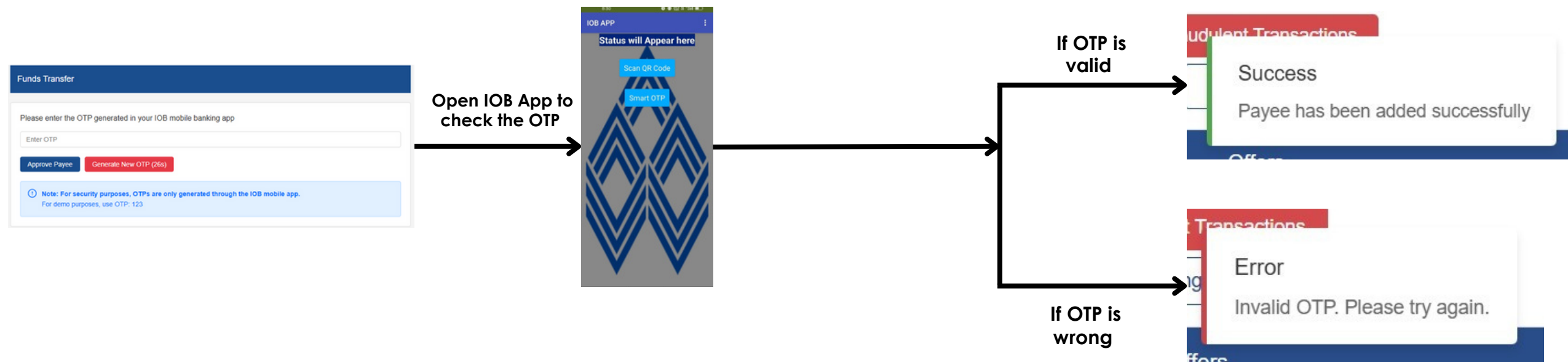
- **Seamless Login:** Adaptive X allows users to securely access the banking website without entering usernames or passwords, using a unique, confidential QR code.
- **QR-Based Authentication:** Each user is assigned a personalized QR code that serves as a secure digital identity for authentication.
- **ATM Integration:** Users can withdraw or deposit money at ATMs by simply scanning their QR code through the IOB mobile application, eliminating the need for physical cards or PINs.

2) FlowAuth x 3) NeuroBehaviour (AI Powered Behavioral Authentication)



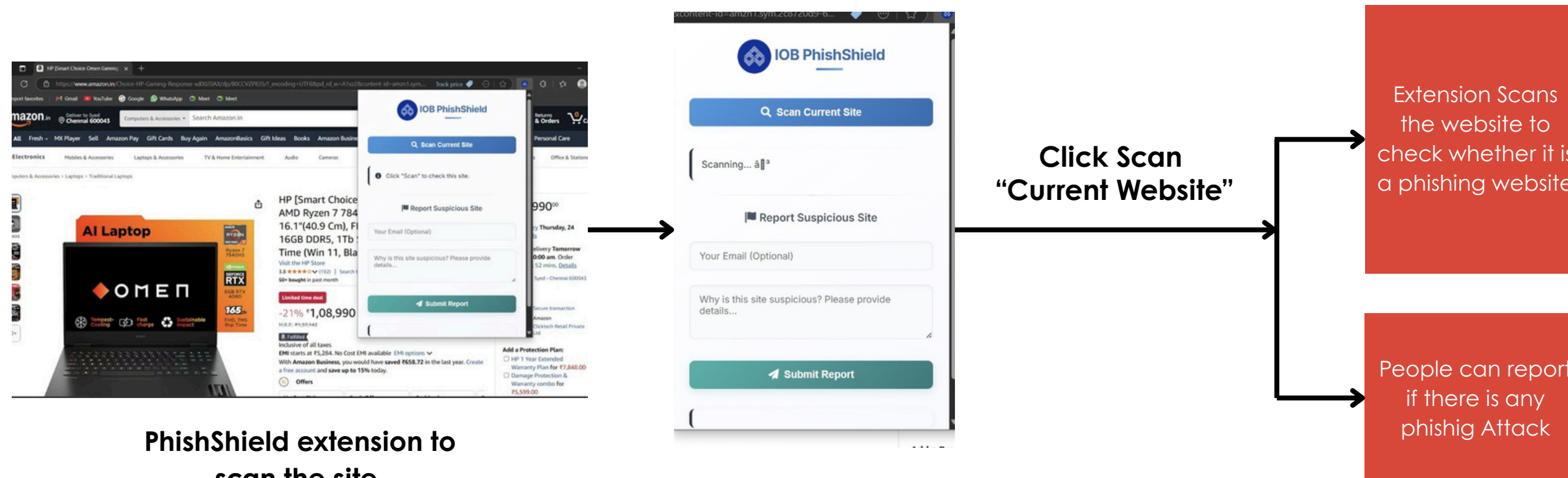
- **Behavioral Analysis:** Neuro Behaviour tracks user-specific interaction patterns like keystrokes and cursor movements to build a behavioral profile.
- **Anomaly Detection:** Unusual behavior triggers anomaly detection, prompting multi-factor authentication to ensure user authenticity.
- **Account Protection:** If multi-factor authentication fails, the session is terminated, preventing unauthorized access and misuse.

4) Smart OTP (Time-Based)



- **Smart Security:** Protects against SMS-based OTP interception.
- **In-App OTP:** Generated within the user account, not via SMS.
- **Time-Based:** Refreshes every 30 seconds for added safety.

5) PhishShield (Web Extension)



- **Real-Time Protection:** Detects and blocks phishing websites instantly.
- **Malicious Site Detection:** Identifies suspicious URLs and behaviors.
- **User Safety:** Protects personal and financial information from theft.



Exception Handlers



FEASIBILITY & VIABILITY

- Technically feasible with software integration, **no additional hardware** required, and open-source models to reduce costs.
- **Automates** threat detection, minimizing manual monitoring. .
- Shifts banking staff focus from **repetitive tasks to more strategic**, human-intensive operations.
- Addresses all three domains: **security, user satisfaction, and behavior analysis.**

Scalable

Secure

Smart

Saves a lot of time



IMPACT

- Revolutionizes **digital identity protection** through continuous, intelligent authentication.
- Reduces reliance on passwords, thereby mitigating risks of **phishing and brute-force attacks**.
- Enables us to attract customers from younger age groups with our smart features.

Benefits:

- a. **Increased security** via AI-driven threat detection.
- b. **User-friendly experience** with adaptive, frictionless login flows.
- c. **Scalable and modular** - easily integrated into various industries (banking, education, healthcare).



Research Papers:

- Anomaly Pattern Detection on Data Streams (2018 DOI: 10.1109/BigComp.2018.00127)
- Research on Time Series Anomaly Detection Algorithm and Application (2019 DOI:10.1109/IAEAC47372.2019.8997819)
- Into the Unknown: Unsupervised Machine Learning Algorithms for Anomaly-Based Intrusion Detection (2020 DOI:10.1109/DSN-S50200.2020.00044)
- A Novel LSTM-GAN Algorithm for Time Series Anomaly Detection (2019 DOI: 10.1109/PHM-Qingdao46334.2019.8942842)
- Credibility of Browser Extension Program Based on Behavioral Statement (2021 DOI: 10.1109/IPEC51340.2021.9421124)

Youtube references :

- <https://youtu.be/YCzL96nL7j0?si=aD7wcp97RgujNv7C>
- https://youtu.be/b1vW0xCto_U?si=HDDsZPJo2uULifYs
- <https://youtu.be/VHx-jpCOASo?si=XAgpFz0VcBI3vWTL>
- <https://youtu.be/n2eT3JRGAM4?si=Y-hahw7UFfOpZjB4>

Reference Articles:

- <https://www.firstbank.com/resources/learning-center/top-banking-trends-to-watch-in-2025/>
- <https://neontri.com/blog/mobile-banking-ux-trends/>
- <https://kissflow.com/solutions/banking/banking-technologies/>
- <https://www.kyndryl.com/us/en/about-us/news/2024/09/financial-services-tech-trends-2024?>