

## **IOB CYBERNOVA HACKATHON 2025**



### Problem Statement Title - Secure Authentication Framework

Theme - Cybersecurity in Banking

**PS Category - Software** 

Team ID - 1

### Team Name - Solution Seekers

Name of the Members and College Regn No:
Jhasim Hassan J - 220071601101, B. Tech CSE
Faheem Khan B - 220171601026, B. Tech AI & DS
Mohamed Iqsan F - 220171601053, B. Tech AI & DS
Mohideen Sathak Uzham J - 220171601074, B. Tech AI &







## PROPOSED SOLUTION



# ZERO TRUST ARCHITECHTURE

#### **Secure Login**

User credentials + OTP + Face guided voice verification

#### **Behavioral Biometrics**

Anomoly detection using user biometric



#### **Zero-Trust Implementation**

No implicit trust is given to the user even after login

#### **AI Risk Scoring**

Previous user data + Validate with current user action

#### **Voice-Guided Facial Verification**

Deepfake and impersonation detection with our model





# FEASIBILITY AND VIABILITY



Feasibility	Key Challenges	Our Solutions
Smaller Development Time compared to other hardware alternatives	Time consuming log in process	Overcome by our AI model which makes the user login easier that's less risky assessed by our model
No Additional Accessories Required	Biometric spoofing	Multi step model. includes user device geolocation, device fingerprint(unique address), keyboard format
Can be easily integrated with existing IOB banking systems	Deepfake Prevention	Video match with person, voice should match User data collected in sign up, lip sync with movement and audio everything assessed by our ML model

Protecting every user, every login — with Zero Trust Architecture - Trust No One, Verify Always!





## **TECHNICAL APPROACH**



In case of unusual sabled

Zero-Trust Architecture enabled

Re-triggering verification methods

Karthik (USA) initiates a bank transfer to his father

Saravanan opens IOB app on his phone in rural Tamil Nadu

Enters Customer ID + Password Saravanan reads 4digit prompt aloud System checks:

- ! Location Typing behavior
- Trusted device
- Any anomaly triggers MFA/block

Access granted →
Transaction confirmed
Karthik gets
notification → IOB logs
activity

Karthik Sends Funds Saravanan Proceeds to Login

OTP Verification

Face + Voice Verification Risk Scoring & Fraud Detection Secure Access & Fund Confirmation

IOB

**Indian Overseas Bank** 

Secure Al Banking

Loading your secure banking experience

Indian Overseas Bank Secure

Indian Overseas Bank O Secure Banking

Please enter your Customer ID to continue

Customer ID

Banking

faheem@gmail.....

Continue

© 2025 Solution Seekers. All rights reserved. Version 1.0.0 Indian Overseas Bank O Secure Banking

**OTP Verification** 

Please enter the 6-digit OTP sent to your registered mobile number

3 4 5 2 2

Resend OTP in 0:50

Verify & Continue

— Back to Password

© 2025 Solution Seekers. All rights reserved. Version 1.0.0 **Facial Recognition Verification** 

Complete the facial and voice recognition challenge for secure access



Please read out loud:

Look directly at the camera and speak clearly

Stop Recording

Feb Mar Apr May Jun

**Risk Assessment Complete** 

Your identity has been verified with low risk score





# **TECHNICAL APPROACH**





#### **Secure Login**

- Uses user ID, OTP, and voice-guided facial verification
- Data safely transferred using HTTP/3 and gRPC protocols for wrapper system



#### **Al Risk Scoring**

- Validates user access based on login history, device trust, IP, location, and behavioral factors
- Dynamically classifies access as safe or suspicious



#### **Behavioral Analysis**

- Compares typing/mouse/touch patterns with past and arbitrary data
- Flags anomalies based on deviation from normal behavior



#### **Voice-Guided Facial Verification**

- · Matches user's facial data from DB
- Validates spoken digits
- · Ensures face and voice sync in real time



#### **Zero Trust Architecture**

- · Every request undergoes risk scoring
- Classified as Low (direct access), Medium (MFA), or High (block + alert)





# **IMPACT AND BENEFITS**



## **IMPACTS**



# Impersonation Protection

It prevents impersonation by matching faces only to those registered during signup. No match, no access.

01



# Spoofing Detection

It tackles spoofing — like holding up a photo or video — by detecting liveness cues such as blinking, slight head movement, or 3D facial structure.

02



#### Deepfake Defense

For deepfake attacks, our model uses feature integrity checks to identify unnatural artifacts that Algenerated faces often leave behind.

03



#### **Cost-Effective**

Unlike hardware
alternatives, we use the
device's camera and mic —
avoiding expensive
installations and
maintenance

01

### **BENEFITS**



# Rapid & Scalable Deployment

Because it's software-based, it can be deployed across thousands of users instantly — from cities to remote towns — without special infrastructure.

02



## Energy Efficient Aligned to SDGs

No extra hardware means lower energy use and ewaste. It's sustainable, inclusive, and aligned with UN SDG goals.

03



# RESEARCH AND REFERENCES



Team 1 Solution Seekers

#### Verizon DBIR 2024 Report

Highlighted that 81% of data breaches involve weak or stolen credentials, inspiring our layered, Aldriven authentication system with Zero-Trust verification.

#### Google Deepfake Research (2023)

We leveraged findings on deepfake detection techniques — like lip-audio sync analysis and visual artifact detection — to train our AI model for face-voice matching accuracy.

#### Proven Technology, Bank-Tested Approach

Inspired by strategies used by Chase (AI Risk Scoring), HSBC (Behavioural Biometrics), and ICICI (Continuous Authentication), tailored specifically for IOB's banking operations.

According to the Federal Reserve Report (2024), financial institutions suffered over \$5 billion in losses due to account takeovers, highlighting the urgent need for advanced, intelligent authentication systems like ours to proactively prevent fraud

Our solution isn't just a project—it's IOB's next-generation security foundation.