अBHYUDAYA

DEPARTMENT OF
COMPUTER SCIENCE AND BUSINESS SYSTEMS

INNOVISION 2025

HACK-SPHERE

Powered by:

FIRMWAY
Automating Confirmation & Reconciliation

Algorand
Bharat

G Soft Solutions

PRIZES WORTH
₹75,000
+
INTERNSHIP OPPORTUNITIES

Team Details

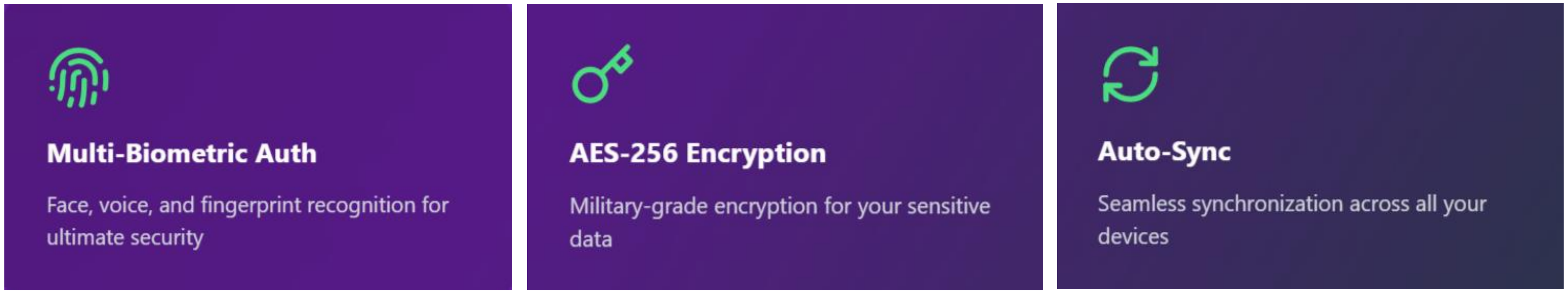
Team name: IgnitedMinds
Team leader name: Prasad Kute
Domain : Security
Problem Statement: Biometric Password Vault

Proposed Solution :

Developing a Cross-platform to securely store, manage, and retrieve passwords using advanced biometric authentication like face, voice and fingerprint recognition. It’s designed to simplify password management while keeping everything safe and synced across devices.

Key Features:

- Integration with Google’s password storage.
- Cross-platform support (Chrome Extension, Android App, Web Interface).



Multi-Biometric Auth

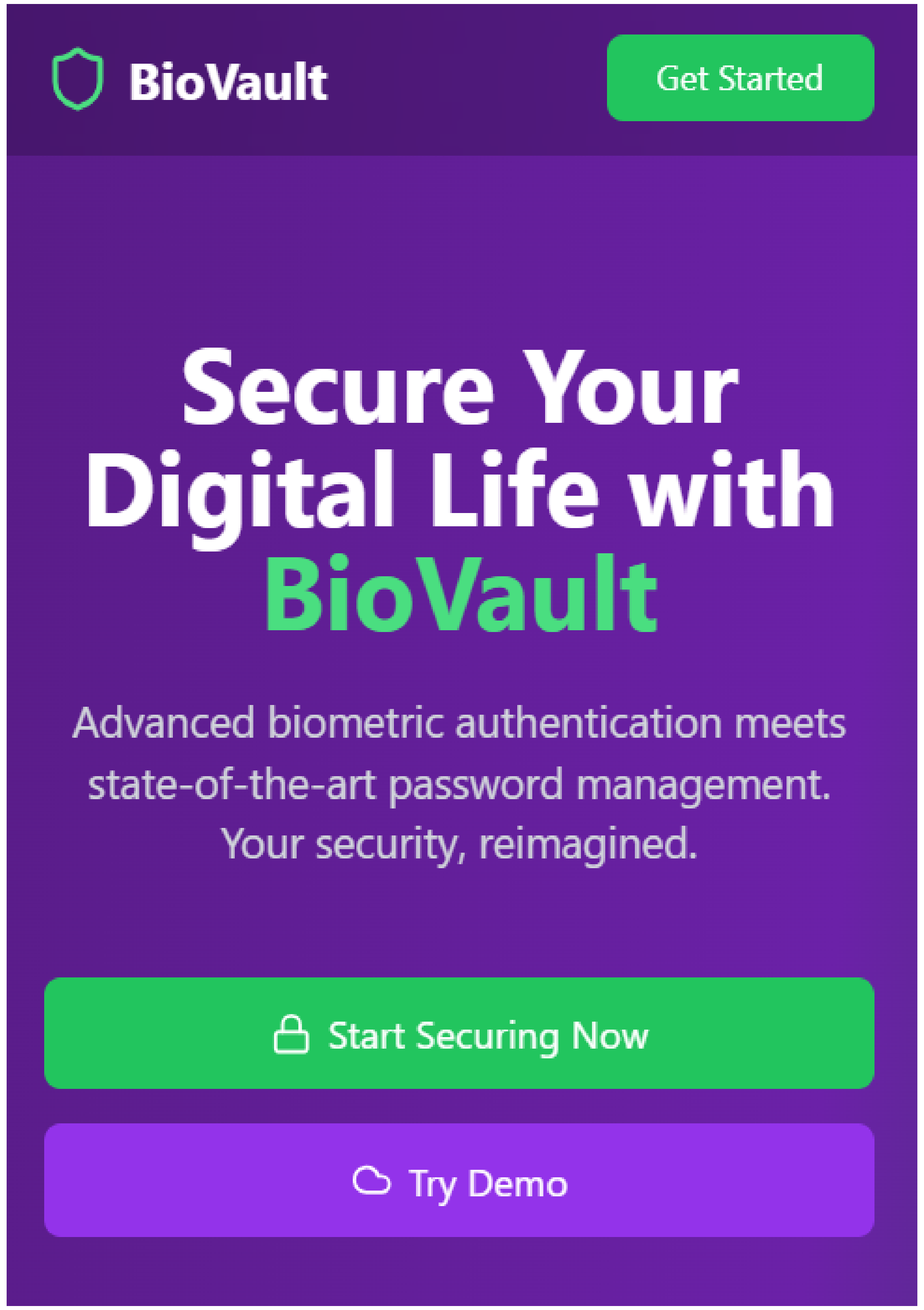
Face, voice, and fingerprint recognition for ultimate security

AES-256 Encryption

Military-grade encryption for your sensitive data

Auto-Sync

Seamless synchronization across all your devices



Secure Your Digital Life with BioVault

Advanced biometric authentication meets state-of-the-art password management. Your security, reimagined.

अBHYUDAYA

FIRMWAY
Automating Confirmation & Reconciliation

HACK-SPHERE

Powered by:

G Soft Solutions

Algorand Bharat

TECHNICAL APPROACH

TECHNICAL INFORMATION

I. **Website using React and FastAPI:** Build a secure password vault with **React** for the frontend and **FastAPI** for the backend.

II. **Authentication & Security:** Integrate biometrics (**voice, fingerprint, photo**) using **WebAuthn, Google APIs,** and **AES-256** encryption. Passwords and metadata stored in **MongoDB**, while encrypted vault files and biometric data are stored on **Cloudinary**.

III. **Cross-Platform:** Develop a React Native **Android** app and a **Chrome extension** for password management.

IV. **Password Management:** Enable secure storage, generation, and retrieval with FastAPI, MongoDB, and AWS integration.

V. **Two-Factor Authentication (2FA):** Add SMS/email-based tokens for extra security during login and transactions.

TECHOLOGY STACK

FastAPI

React

GitHub

mongoDB

AES-256 ENCRYPTION

tailwindcss

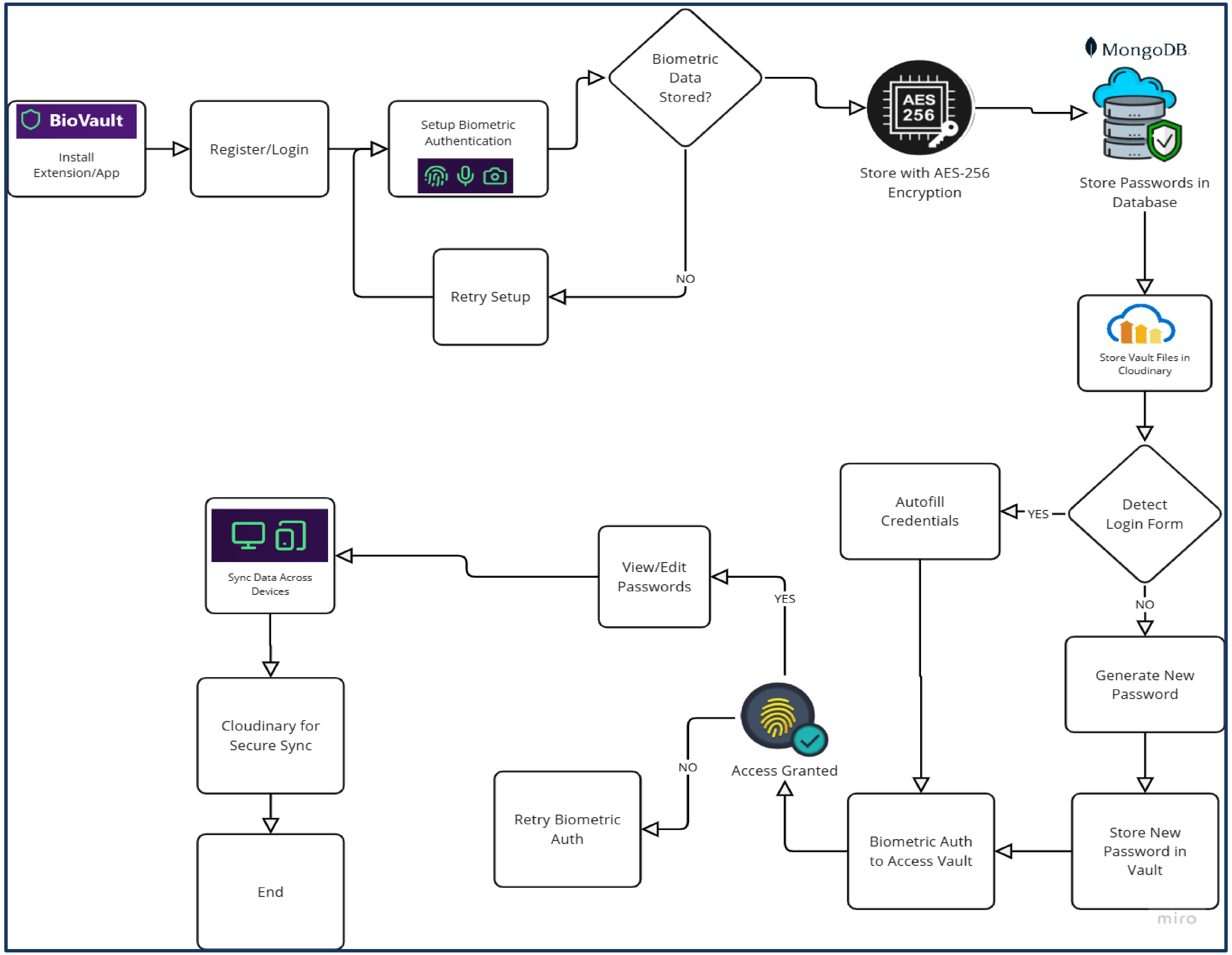
Chrome Extension

Google APIs

GIT

Android App

Cloudinary



BioVault
Install Extension/App

Register/Login

Setup Biometric Authentication

Biometric Data Stored?

NO

Retry Setup

Store with AES-256 Encryption

MongoDB

Store Passwords in Database

Store Vault Files in Cloudinary

Detect Login Form

YES

Autofill Credentials

NO

Generate New Password

Store New Password in Vault

Biometric Auth to Access Vault

Access Granted

NO

Retry Biometric Auth

YES

View/Edit Passwords

Sync Data Across Devices

Cloudinary for Secure Sync

End

अBHYUDAYA

FIRMWAY
Automating Confirmation & Reconciliation

HACK-SPHERE

Powered by:

G Soft Solutions

Algorand
Bharat

UNIQUENESS AND NOVELTY

Feature	BioVault	1Password	LastPass	bitwarden	KEEPER
Password Generation	✓	✓	✓	✓	✓
Multi-Factor Authentication	✓	✓	✗	✗	✗
Cross-Platform Support	✓	✓	✓	✓	✓
Voice Authentication	✓	✗	✗	✗	✗
Fingerprint Authentication	✓	✓	✓	✓	✗
Photo Authentication	✓	✗	✗	✓	✓
Auto Login Form Filling	✓	✓	✓	✓	✓
Browser Extention Available	✓	✗	✗	✗	✓
TOTP Generation	✓	✓	✓	✓	✓

Unique Value Proposition (UVP) for BioVault

1.Triple-Biometric Security: Industry-leading multi-biometric authentication with voice, fingerprint, and photo recognition for unparalleled protection and convenience.

2.Seamless Multi-Platform Integration: Access your vault securely across a website, Android app, and Chrome extension with unified, user-friendly functionality.

3.Cutting-Edge Backend: Built using **FastAPI** for lightning-fast performance, scalability, and secure API interactions, paired **Cloudinary** with for encrypted data storage.

4.Enhanced Security with TOTP: Native integration of Time-Based One-Time Passwords (TOTP) ensures an extra layer of security for your accounts.

5.Advanced Encryption Standards: We employ AES-256 encryption, a higher standard than the commonly used ChaCha20, ensuring top-tier security for user data.

6.User-Centric Design: Our platform offers a seamless and intuitive user experience across multiple platforms, ensuring accessibility and ease of use.

7.Future-Ready Technology: Embracing multi-biometric authentication positions our solution at the forefront of security technology, catering to evolving user needs and preferences.

FEASIBILITY AND VIABILITY

Technical Feasibility:

- **Technology Availability:** APIs like Google Speech-to-Text, WebAuthn, and BiometricPrompt are accessible for biometrics.
- **Security:** AES-256 encryption and HTTPS ensure secure data handling.
- **Compatibility:** MERN stack and React Native/Kotlin enable scalable, cross-platform development.

Operational Feasibility:

- **Team:** Developers, security experts, and UX designers needed for implementation.
- **Scalability:** Cloud infrastructure like Firebase or AWS supports growth.

Market Feasibility:

- **Demand:** Increasing need for secure password management solutions.
- **Accessibility:** Multi-biometric authentication simplifies user access and improves adoption.
- **Revenue Model:** Freemium plans attract users; subscriptions provide advanced features.

Potential Challenges	Strategies to Overcome:
Technical Risks: Data security concerns and vulnerabilities in APIs and cloud services.	**Technical Solutions:** Conduct regular security audits and provide offline access features.
Operational Risks: Server downtime during peak usage.	**Operational Readiness:** Partner with reliable cloud providers to ensure uptime and data security.
Market Risks: Resistance to adopting new biometric technology.	**Market Strategies:** Run webinars and tutorials to educate users and improve adoption rates.

Team Details

Name	Email	Phone Number
Prasad Rajaram Kute	Prasad.22210330@viit.ac.in	7558750366
Arya Jalindar Kadam	arya.22210766@viit.ac.in	8779831758
Chinmay Ashok Kale	chinmay.22210926@viit.ac.in	9021658271
Tejaswini Jaywant Durge	tejaswini.22210270@viit.ac.in	8446528408