

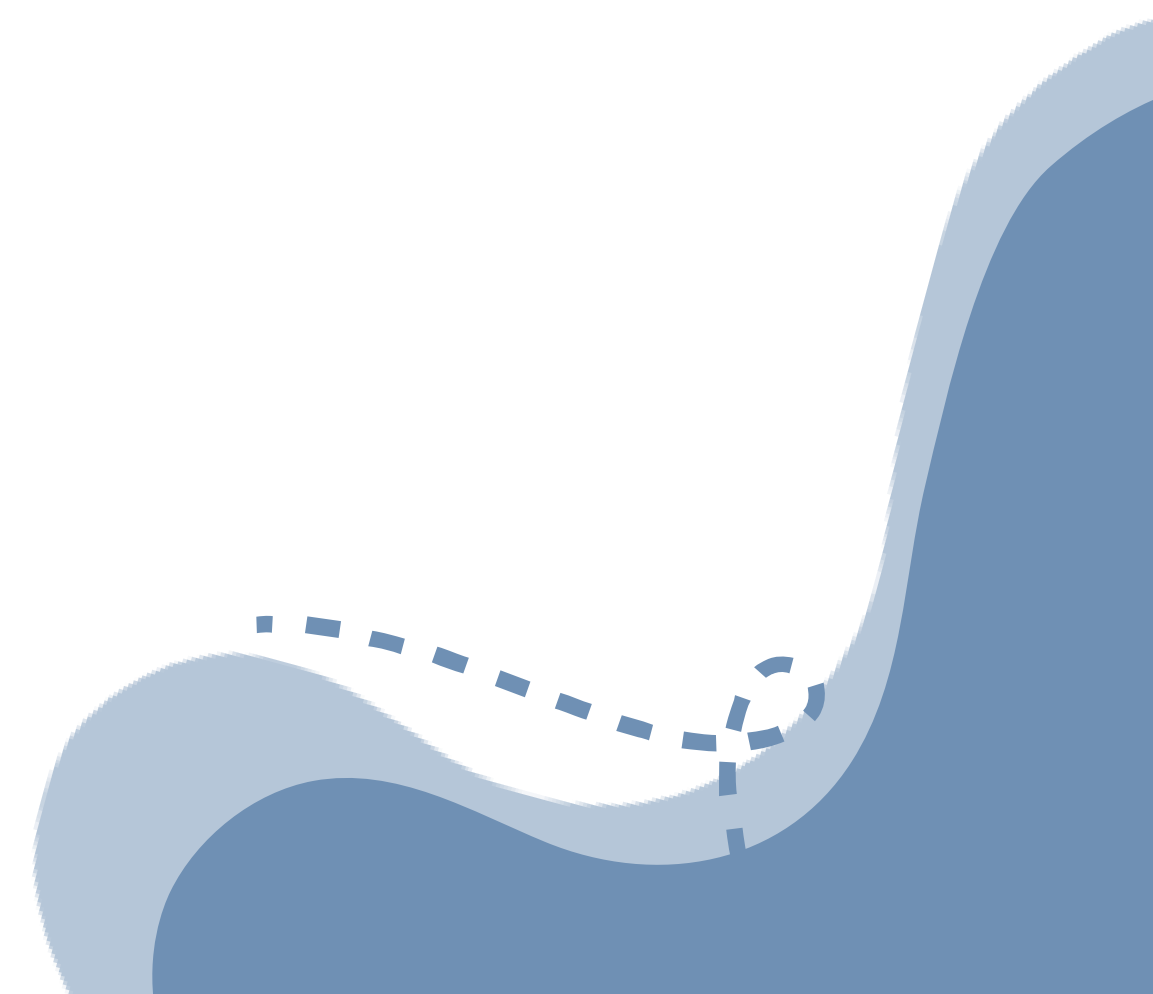


FINTECH HACKATHON FOR SRM GROUP OF INSTITUTIONS



MULTI-BIOMETRIC AUTHENTICATION:
A SECURE ALTERNATIVE TO OTP USING FACIAL AND
VOICE RECOGNITION FOR DIGITAL TRANSACTIONS

OUR TEAM:

1. Akshit Bhatt
 2. Abhay Kumar
 3. Vishnu Gupta
- 

ABSTRACT

- In the digital age, secure transaction authentication is crucial. Traditional methods like One-Time Passwords (OTP) are becoming vulnerable to security threats such as phishing and SIM swapping, while also adding inconvenience for users.
- Our project proposes an alternative: a multi-biometric authentication system that uses facial and voice recognition to verify users. By relying on unique biometric traits, this method offers stronger security and a more seamless user experience. This approach reduces the risks associated with OTPs and enhances the overall safety of digital transactions.

MARKET ANALYSIS

- The digital transaction market is experiencing rapid growth, with billions of transactions processed daily in sectors like e-commerce, banking, and fintech. However, traditional methods such as One-Time Passwords (OTP) are increasingly vulnerable to phishing, SIM swapping, and other security threats, driving the need for more secure alternatives.
- The global biometrics market is expanding significantly, with facial and voice recognition becoming preferred solutions due to their accuracy and convenience. Industries such as finance, healthcare, and government are adopting biometrics for fraud prevention and regulatory compliance.
- Our multi-biometric authentication system directly addresses this demand by offering a more secure and seamless alternative to OTP, making it highly relevant for sectors requiring reliable digital transaction authentication.

CONSUMER AQUISITION

The demand for secure, convenient authentication methods is growing, particularly in industries such as banking, e-commerce, healthcare, and government services. To attract consumers, we will:

1. Target high-risk sectors (like finance and fintech) where secure authentication is crucial.
2. Leverage partnerships with financial institutions and digital service providers that require enhanced security solutions.
3. Offer competitive pricing and seamless integration with existing transaction systems to encourage early adoption.
4. Utilize a freemium model for smaller organizations and premium features for enterprise-level clients.
5. Implement educational campaigns highlighting the security risks of OTP and the benefits of biometric authentication.

VIABILITY

Our multi-biometric system is designed to be:

1. **Scalable** – Easily adaptable to different platforms, including mobile, web, and desktop applications.
2. **Cost-effective** – By using widely available biometric technologies (facial and voice recognition), the implementation costs remain low.
3. **Highly secure** – Biometric data is unique to each user, reducing the risk of fraud and making it a viable long-term alternative to OTP-based systems.
4. **User-friendly** – Biometrics offer a seamless, one-step authentication process, improving the user experience compared to traditional methods.
5. **Sustainable** – With the growing demand for strong authentication in various sectors, the adoption of multi-biometric systems will continue to increase, ensuring the long-term viability of the application.

TECH-STACK

Frontend---

- HTML5: For structuring web pages.
- CSS3: For styling.
- JavaScript: For client-side logic.
- React.js: For building dynamic user interfaces.

Backend---

- Python: Main language for handling backend logic and biometric processing.
- Flask or Django: Web frameworks for building RESTful APIs (Flask is lighter, Django is more feature-rich).
- PyMongo: MongoDB driver for Python to interact with MongoDB.

Biometric Authentication---

Facial Recognition

- OpenCV: For image processing and face detection.
- Dlib: For facial landmark detection and face recognition.
- Face recognition: High-level library for facial recognition tasks (built on top of Dlib).

Voice Recognition

- Google Speech-to-Text API : For converting speech to text.
- Deep Speech: For speech recognition using deep learning.
- PyDub : For audio signal processing.

TECH-STACK

Database---

- MongoDB: NoSQL database for storing user data and biometric information.
- PyMongo: For interacting with MongoDB from Python.

Authentication and Security---

- JWT (JSON Web Tokens): For managing secure user sessions.
- Flask-JWT-Extended or Django Rest Framework JWT: For implementing JWT in Flask or Django respectively.
- bcrypt: For securely hashing user passwords

ROADMAP FROM TECHNOLOGY TO BUSINESS

- The journey begins with research and planning over the first 1-2 months to understand market needs and finalize the technology stack, including Python and MongoDB. During the prototype development phase (3-4 months), the focus shifts to building the backend, integrating biometric features, and developing the frontend using React.js.
- Following this, the testing and refinement stage (5-6 months) involves thorough system and user testing to ensure functionality and user satisfaction. The final phase of deployment and launch (7-8 months) includes deploying the application to cloud platforms and officially launching it while monitoring performance.
- In the business strategy phase, starting from month 9, efforts will focus on market entry through targeted marketing and sales strategies, along with setting up customer support. As the business scales (months 11-12), the focus will be on expanding features, geographic reach, and optimizing performance.
- The monetization strategy (months 13-14) will involve implementing a pricing model and exploring revenue streams, followed by ongoing efforts in sustainability and innovation (15+ months) to continuously improve the product and plan for long-term growth.