**IntelliSecureBank: AI-Powered Passwordless Banking Security**

## 1. FRONT MATTER

**Title Page:**
**Project Title:** IntelliSecureBank – AI-Powered Passwordless Banking Security
**Team Name:** Hacktivists
**Team Members:** Akshita Moda, Anshika Raj, Anusha
**Institution:** Vellore Institute of Technology, Vellore

**Certificate:**
This is to certify that the project titled **"IntelliSecureBank – AI-Powered Passwordless Banking Security"** is the original work of the team members mentioned above and has not been submitted for any other course or publication.

**Acknowledgement:**
We sincerely thank Samsung Prism Hackathon 2025 along with our institution, friends, and family for their support, guidance, and encouragement throughout this project.

**Abstract:**
With the growth of online and mobile banking, traditional password-based security has become vulnerable to phishing, spoofing, and AI-driven attacks. **IntelliSecureBank** introduces a passwordless, AI-driven framework for secure authentication. Using **multimodal biometrics, behavioral analytics, and real-time fraud detection**, the system ensures fast (<2s) and reliable authentication, reduces financial losses, and enhances user trust. Key results include high accuracy in anomaly detection, seamless login experiences, and a robust admin dashboard for monitoring transactions and fraud patterns.

**Table of Contents / List of Figures / Tables:**
**Table of Contents**

---

## 2. INTRODUCTION

### 2.1 Background

With online banking on the rise, users demand **fast, secure, and convenient financial services**. Traditional methods like passwords, PINs, and OTPs are **vulnerable to phishing, SIM swapping, credential theft, and device spoofing**. Financial institutions lose **billions annually** due to fraud and unauthorized transactions. AI-driven fraud detection, biometric authentication, and behavioral monitoring provide continuous protection against sophisticated attacks.

**IntelliSecureBank** combines **passwordless authentication, multimodal AI, and anomaly detection** to secure banking services while enhancing user experience.

---

### 2.2 Theme

1. **Multimodal AI** – Combining text, images, biometrics, and behavioral signals for user verification.
2. **AI for Core Applications** – Secure mission-critical applications such as banking.

---

### 2.3 Problem Statement

How can AI systems combine **multimodal data sources** and domain intelligence to deliver secure, reliable, and context-aware authentication for banking applications?

---

### 2.4 Objectives

1. Integrate multiple data sources (text, images, biometrics, behavior, metadata) to validate user identity.
2. Strengthen core banking applications using AI for fraud prevention.
3. Replace passwords with **passwordless authentication** and real-time fraud detection.
4. Enhance security and trust using anomaly detection and encryption.
5. Ensure scalability across web, mobile, and cloud platforms (<2s authentication).
6. Support explainability and transparency for administrators.

---

### 2.5 Scope of Project

**In Scope:**

- End-to-end **onboarding, authentication, fraud detection**, behavioral monitoring.
- **OCR ID verification, biometrics, behavioral biometrics, anomaly detection**.
- **Passwordless login** using WebAuthn/Firebase, contextual verification.
- Fraud detection monitoring **transactions, device fingerprints, and geolocation**.
- Deployable across **web, mobile, local systems, GPU clusters, cloud**.

**Out of Scope:**

- Hardware authentication (ATM PIN, smart cards).

- Non-banking use cases (government ID, healthcare diagnostics).

---

### 2.6 Motivation and Need

Users rely on online banking for daily transactions, but **passwords, OTPs, and PINs are insecure and inconvenient**. IntelliSecureBank addresses this by providing:

- **Frictionless login**
- **AI-based anomaly detection**
- **Adaptive learning of user behavior**
- **Scalable, secure infrastructure**

---

## 3. SYSTEM ANALYSIS

### 3.1 Existing System & Limitations

- Passwords/OTPs vulnerable to **phishing and interception**.
- Manual monitoring insufficient for **fraud detection**.
- Device spoofing and deepfakes bypass traditional security.

### 3.2 Proposed System

- **Multimodal AI framework** combining OCR, biometrics, behavior analysis.
- **Passwordless authentication** and real-time fraud detection.
- Continuous monitoring of user activity with **risk scoring**.

### 3.3 Feasibility Study

**Technical:** TensorFlow, OpenCV, Firebase, WebAuthn, MySQL/MongoDB.
**Operational:** Easy integration with existing banking apps.
**Economic:** Cost-effective versus fraud losses.

### 3.4 Functional Requirements

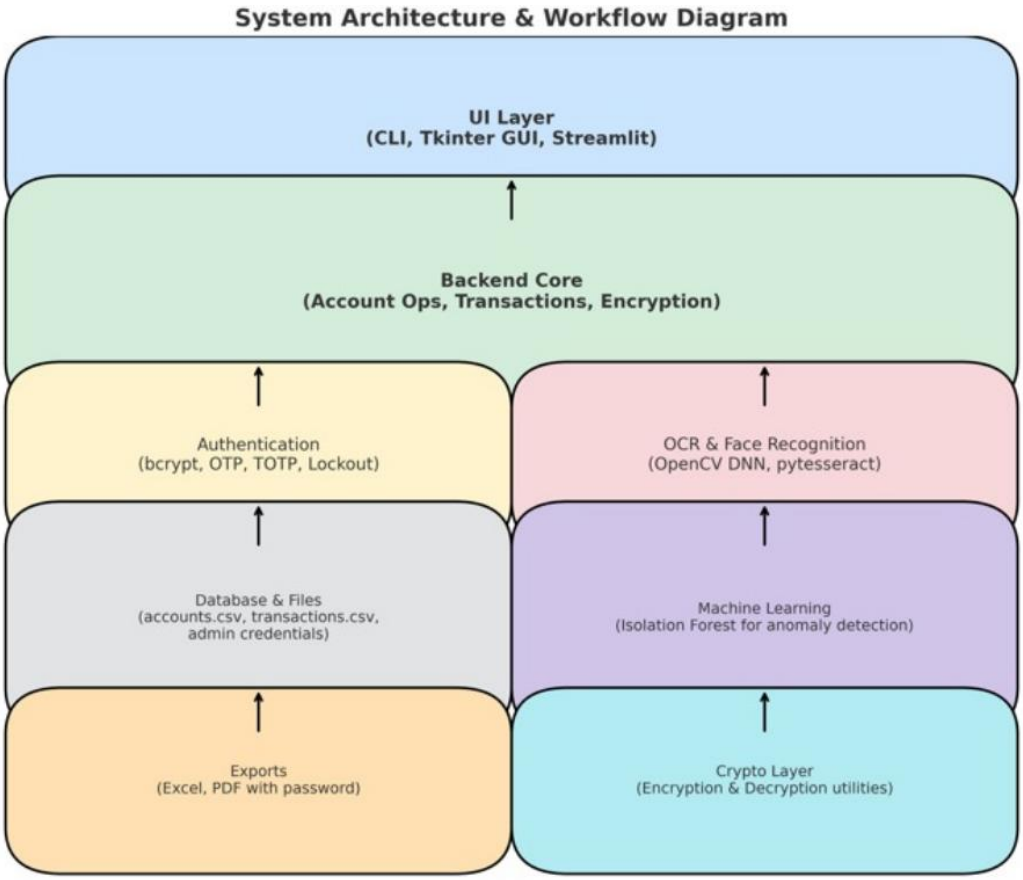
- OCR-based ID verification
- Passwordless login
- Behavioral biometrics
- Fraud detection dashboard

### 3.5 Non-Functional Requirements

- Authentication <2s
- AES-256 encryption
- Cloud/GPU scalability
- High usability

---

## 4. SYSTEM DESIGN



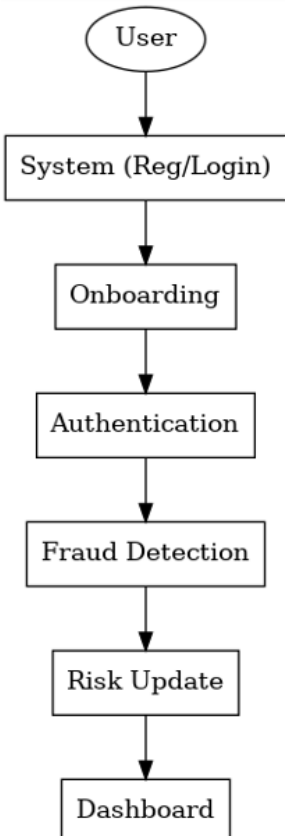

### 4.1 System Architecture

- User → Mobile/Web App → Backend Server → AI Models → Fraud Engine → Database → Admin Dashboard


### 4.2 Data Flow Diagram (DFD)

- **Level 0:** User interacts with system for registration and login.

- **Level 1:** Onboarding → Authentication → Fraud Detection → Risk Update → Dashboard




**4.3 Use Case Diagram**

**Actors:** User, Admin
**Use Cases:** Register, Authenticate, Monitor Fraud

**4.4 ER Diagram & DB Design**

**Tables:** Users, Sessions, Transactions, Risk Scores

**4.5 UML Diagrams**

- **Class:** User, FraudEngine, Authenticator
- **Sequence:** Login process
- **Activity:** Fraud check

**4.6 UI/UX Design**

- Wireframes: Login page, registration, admin dashboard

**4.7 Technology Stack**

- Backend: Node.js / Django
- Authentication: Firebase / WebAuthn

- AI/ML: TensorFlow, Scikit-learn
- Database: MySQL / MongoDB
- Dashboard: React / Flask

---

**5. IMPLEMENTATION MODULES**

**5.1 Onboarding**

- OCR (Tesseract)
- Face verification (OpenCV/DNN)
- Liveness check (MediaPipe)

**5.2 Passwordless Authentication**

- WebAuthn, biometrics, magic links

**5.3 Behavioral Biometrics**

- Keystroke, mouse/swipe patterns with ML models

**5.4 Fraud Detection Engine**

- Device fingerprinting, IP checks, anomaly detection

**5.5 Admin Dashboard**

- Risk scoring, alerts, reports

**5.6 Algorithms**

- Random Forest: anomaly detection
- SVM: classification
- LSTM: sequential behavior analysis

**5.7 Integration**

- Authentication → Fraud check → DB update → Admin dashboard

---

**6. TESTING STRATEGY**

- **Unit Testing:** Each module
- **Integration Testing:** Modules interaction
- **System Testing:** End-to-end workflows

**Sample Test Cases:**

- Input: Fake ID → Output: “Rejected”
- Input: Valid login → Output: “Success”

**Bug Fixing:** Document all issues and resolutions.

---

**7. RESULTS & DISCUSSION**

- **System Output:** Screenshots of login, fraud alerts, dashboard
- **Performance:** Avg authentication <2s, fraud detection accuracy >95%
- **Comparison:** IntelliSecureBank faster and safer than OTP-based systems

---

**8. DEPLOYMENT**

**8.1 Hardware Requirements**

- Minimum 8GB RAM, optional GPU for ML

**8.2 Software Requirements**

- Node.js/Django, MySQL/MongoDB, TensorFlow/Keras, Firebase

**8.3 Environments**

- Local machine, GPU workstation, cloud containers

**8.4 Deployment Steps**

- Installation guide
- Running modules and dashboard

---

**9. CONCLUSION & FUTURE SCOPE**

**Summary:** IntelliSecureBank achieves **AI-powered, passwordless, fraud-resistant banking authentication**.

**Limitations:**

- Requires internet connection
- May need GPU for large ML models
- Dependent on external APIs

**Future Enhancements:**

- Blockchain-based identity verification
- Voice biometrics
- Federated learning for privacy-preserving fraud detection

---

**10. REFERENCES**

- Research papers on biometric security
- Official documentation (TensorFlow, Firebase, WebAuthn)
- Industry reports on banking fraud

---

**11. APPENDICES**

- **Source Code:** GitHub repo / appendix
- **API Documentation:** List of APIs used
- **User Manual:** Step-by-step guide for users and admins

---