Special Features Explaination

To protect user accounts, prevent illegal access, and maintain platform trust, the Rentverse mobile app implements an advanced login security and anomaly detection system. We have 5 special features which is security check during login, multiple failed login attempt detection, suspicious location detection, abnormal login time detection and suspicious login alert & monitoring.

1. Security Check During Login

Every login request is validated through multiple security checks before access is granted.

What the system checks:

- Correct username/email and password
- Valid authentication token
- Device and session verification

Purpose:

- Prevent unauthorized users from accessing accounts
- Ensure only verified users can enter the system

2. Multiple Failed Login Attempt Detection

The system monitors the number of failed login attempts for each user.

How it works:

- If a user fails to log in **more than 5 times consecutively**:
    - The account is temporarily locked **OR**
    - A security alert is triggered
- The user may be required to:
    - Wait for a cooldown period
    - Verify identity (e.g., OTP or admin review)

Purpose:

- Protect against brute-force attacks
- Reduce password-guessing attempts

3. Suspicious Location Detection

RentVerse checks the **geographical location** of each login attempt.

How it works:

- Compares current login location with:
    - Previous login locations
    - Usual user activity region
- Flags logins from:
    - Different countries
    - Unusual or unknown locations

System action:

- Marks the login as suspicious
- Sends an alert to the admin or user
- May require additional verification

Purpose:

- Detect account hijacking
- Prevent access from unauthorized regions

4. Abnormal Login Time Detection

The system analyzes login time patterns for each user.

Examples of abnormal behavior:

- Login at **unusual hours** (e.g., 3–5 AM)
- Login time differs significantly from normal user behavior

System response:

- Flags the activity as abnormal
- Logs the event for monitoring
- May trigger a security alert

Purpose:

- Identify compromised accounts
- Enhance behavioral-based security

5. Suspicious Login Alert & Monitoring

All suspicious activities are logged and monitored in real time.

Features include:

- Login activity logs (time, location, device)
- Automated alerts for abnormal behavior
- Admin dashboard for security monitoring

Purpose:

- Enable quick response to security threats
- Support auditing and incident investigation