Security Measures that we maintain for our Agent Banking System:

1. Agent Banking system runs on a private network (no access from Internet); only accessible through secure VPN connection from both Agent Point and Branch, HO.

2. All data communication between Agent Point devices (mobile and computer) and the server is encrypted using Transport Layer Security (TLS, https). This encrypted data stream is also sent over VPN tunnel.

3. Only port 443 is open on the server for inbound data traffic.

4. VMs are only accessible from within the bank's private network and only from white listed IPs.

5. Outbound traffic to approved 3rd party services (ie. utility services, telcos, etc.) go through forward proxy (to restrict what can be reached). ABS to forward proxy data traffic is transported over VPN.

6. Built on industry best practice using spring framework and spring security.
    a. Preventions
        i. Authentication Attacks: Prevents brute-force attacks and credential stuffing.
        ii. Authorization Attacks: Guards against unauthorized access and privilege escalation.
        iii. Cross-Site Request Forgery (CSRF) Attacks: Provides automatic CSRF token generation and verification.
        iv. Cross-Site Scripting (XSS) Attacks: Offers built-in protection with input sanitization and Content Security Policy (CSP) support.
        v. Clickjacking Attacks: Supports X-Frame-Options and Content-Security-Policy headers to prevent clickjacking.
        vi. Session Attacks: Mitigates session fixation, hijacking, and concurrency issues with robust session management.
        vii. SQL Injection Attacks: Used parameterized queries, input validation for preventing SQL injection attack.
        viii. Data Breach Prevention: Supports secure password storage and authentication mechanisms to prevent the compromise of user passwords in the event of a data breach.

7. Strict monitoring on user activity

8. Strict monitoring on sql query log

9. Automatic Session Expiration
   Access token, Refresh Token automatically expires after specified period even if the user is active

10. Single Session Maintain
    Single session per user. User's' previous session will be invalidated if the user tries to login from a different app/web.

11. Access Token validation on every API Call

12. Role based authentication and authorization

13. Secure Password Storage and Hashing Mechanism Utilizing Sha256 Algorithm
    a. The chosen algorithm for password hashing, referred to as Sha256, is widely recommended and known for its security properties and irreversible encryption.
    b. The resulting hash, along with the salt, is securely stored in the application's database. This means that the original passwords are never stored directly, providing an additional layer of protection.

14. A CBS Middleware Interface is run on an isolated VM (on private network) for secure connectivity to Bank CBS.

15. Database backup is held every night to transfer to a remote server.

16. Multiple load balanced micro service instances running ensuing high availability and resilience.

17. Each and every transactions are authenticated and authorized by 2FA
    a. Bank issued card with QR code is scanned
    b. Customer's photo is verified by agent/teller
    c. Customer's fingerprint is matched

18. Each transaction is pre-processed where business validation, transaction profiles are checked and then processed when authenticated by fingerprint match.

19. Transaction request integrity is checked by creating a hash during pre-process and checked again during processing of the transaction.