



CASE STUDY

Innait IMPLEMENTATION

TWO-FACTOR AUTHENTICATION (2FA) IN A SCHEDULED
COMMERCIAL BANK

INDUSTRY - BANKING, FINANCIAL SERVICES AND INSURANCE



www.innait.com

Background: A Scheduled Commercial Bank and one of the oldest private sector banks in India, incorporated in 1938

Objective: To bolster security measures and safeguard critical applications, the bank aimed to implement Two-Factor Authentication (2FA) using biometrics. The objective was to enhance security and mitigate risks associated with single-factor authentication methods, such as password-based systems.

Existing System: The bank relied on Single-Factor Authentication (SFA), primarily utilizing passwords to protect its critical applications. However, the inherent vulnerabilities of password-based systems, including password theft and susceptibility to external hacking, prompted the bank to seek a more robust security solution.

Requirement: The bank outlined the following requirements for the implementation of 2FA:

1. **Regulatory Compliance:** The solution must adhere to regulatory standards, particularly the guidelines issued by the Reserve Bank of India (RBI), ensuring compliance with industry regulations.
2. **Biometric Performance:** Biometric comparison must meet stringent performance benchmarks, including rapid fingerprint comparison times for each transaction and overall transaction duration.
3. **Data Security:** Fingerprint templates must be securely encrypted to prevent unauthorized access and ensure data confidentiality.

4. **Scalability:** The solution should be scalable to accommodate multiple instances and variations of the company's critical applications seamlessly.
5. **Integration:** Seamless integration with existing client-server and browser-based environments is essential to minimize disruption to operations.

Solution Deployed: Precision Biometric proposed InnaIT Framework Applications to be integrated with solutions & to provide the required Biometric based two factor authentications for application login.

InnaIT 2FA: The solution is designed to integrate the Biometric solution in a client server/browser-based environment. 2FA solution consists of the below mentioned four components:

1. **Client Driver:** Installed on every client system, the client-side driver facilitated fingerprint capturing and extraction processes.
2. **Server Component:** Housed the fingerprint comparison components in environments such as Microsoft.NET and Java, ensuring robust authentication.
3. **Software:** InnaIT-2FA software facilitated seamless integration and operation of the 2FA solution.
4. **Hardware:** Fingerprint scanners were connected to every PC and thin client via USB ports, enabling biometric enrollment and verification.

Enrollment involved scanning individual fingerprints, with captured data stored as digital templates in the central server. During verification, users' fingerprints were compared to previously registered templates for authentication. The one-to-one matching process ensured secure and reliable authentication without compromising data privacy.

Benefits: The implementation of InnaIT Framework Applications for 2FA provided the bank with the following benefits:

1. **Enhanced Security:** By integrating biometric authentication, the Bank significantly strengthened security measures, reducing the risk of unauthorized access and data breaches.
2. **Regulatory Compliance:** The solution ensured compliance with RBI guidelines and other industry regulations, mitigating regulatory risks.
3. **Improved Audit Trail:** Detailed logs of authentication activities facilitated robust audit trails, enabling effective monitoring and analysis for compliance and security purposes.

4. **Future-Ready Architecture:** InnalT Framework solution offered scalability and flexibility, allowing the bank to adapt to evolving security threats and regulatory changes effectively.

In conclusion, the implementation of 2FA using biometrics via the InnalT Framework Applications provided the bank with a robust security solution tailored to its critical applications, ensuring compliance, confidentiality, and enhanced protection against evolving cyber threats.

X---X