बैंक ऑफ़ बड़ौदा
Bank of Baroda

PSB HACKATHON SERIES 2025

Hackathon Journey Summary: The Intelligent API Security Fabric

Team Name: 200_OK

Team Member: Madhav Lata

Event: Bank of Baroda Hackathon, in association with IIT Kanpur & SIIC

1. Overview of the Problem Statement and its Relevance to Banking

The problem statement, "Zero Trust API Security & Third-Party Risk Management," is not just a technical challenge; it represents one of the most critical and pressing concern facing the modern banking sector. The entire Open Banking revolution is built upon APIs, which act as the digital bridges connecting banks like Bank of Baroda to a vibrant ecosystem of fintech partners.

However, this proliferation of APIs has outpaced the evolution of traditional security. The old "castle-and-moat" model is obsolete in a world where the network perimeter is constantly expanding with each new partner. The industry's reliance on standard Bearer Tokens for authentication has created a foundational security flaw. As industry reports consistently show, stolen credentials are the root cause of over 60% of data breaches. For a bank, a single stolen API token from a compromised partner can translate directly into unauthorized transactions, massive financial fraud, and a catastrophic loss of customer trust. The relevance is therefore immediate and severe: securing these API connections is fundamental to the future success and stability of digital banking.

2. Description of the Solution Developed by the Team

To address this challenge, I developed **"The Intelligent API Security Fabric,"** a working prototype of a multi-layered, Zero-Trust API gateway. The philosophy is simple: **never trust, always verify**. The fabric acts as a single, intelligent entry point for all API traffic, ensuring every request passes through a rigorous security gauntlet before it can reach the bank's core systems.

Our solution is built on three synergistic layers of innovation:

1. **Layer 1: Unphishable Identity:** We make stolen API tokens worthless by cryptographically binding them to a specific application's certificate using Mutual TLS (mTLS) and the IETF RFC 8705 standard for Certificate-Bound Tokens.

2. **Layer 2: Proactive Shield:** We move beyond static firewalls to a dynamic, behavioral analysis engine. The system learns the "normal" rhythm of each API client and can detect and block sophisticated, zero-day attacks (like fuzzing) that would be invisible to traditional defenses.
3. **Layer 3: Zero-Knowledge Privacy:** Leveraging cutting-edge cryptography (zk-SNARKs), we've built a system that can verify sensitive customer data (e.g., "Is this customer over 18?") without the data ever leaving the bank's secure perimeter. This is the ultimate form of data minimization, designed for the era of stringent data privacy laws like the DPDP Act.

3. Highlights of the Team's Journey Through the Hackathon Process

The journey of building the Intelligent API Security Fabric was a challenging yet incredibly rewarding sprint of rapid learning and problem-solving.

The Initial Spark: The hackathon began with an intensive brainstorming phase. I was determined to tackle not just one aspect of API security, but to build a holistic, end-to-end solution. The decision to incorporate Zero-Knowledge Proofs was an ambitious one, but I believed it was the key to a truly innovative project.

The Hurdles: The path was not without its technical obstacles.

- **The Cryptography Challenge:** Implementing the ZKP layer was the most demanding part. Debugging Circom circuits and understanding the nuances of the Groth16 proving scheme required a deep dive into advanced cryptography under a tight deadline. There were several moments where compilation errors seemed insurmountable.
- **The Frontend Integration:** Creating a visually compelling and intuitive frontend to demonstrate these complex backend concepts was crucial. Moving from a static design to the animated, responsive "API Health Orb" involved several iterations to get the feel just right, including overcoming initial build issues with styling frameworks.

The Breakthrough Moments: The most exhilarating moment was seeing the first successful Zero-Knowledge Proof verification come back to the frontend. It was the point where the most ambitious part of the project became a reality. Another highlight was the successful demo of the Layer 2 Proactive Shield, watching the "orb" turn red and the automated "shield" activate—transforming a complex security concept into a simple, powerful visual story.

4. Role of the Bank/IIT Kanpur/SIIC in Supporting the Team

The environment and support provided by the event organizers were instrumental to the success of this project.

- **Bank of Baroda:** By providing a problem statement that is deeply relevant to the real-world challenges in the financial industry, Bank of Baroda gave this project a clear sense of purpose. The mentorship sessions and the opportunity to think about security from a bank's perspective were invaluable in shaping the solution's strategic direction.

- **IIT Kanpur & SIIC:** The infrastructure, environment, and seamless organization of the hackathon at the IIT Kanpur campus created an ecosystem ripe for innovation. Also continuous support from Shagun maám from SIIC was really helpful resolving my queries at the earliest for smooth conduction.

6. Notable Outcomes, Learnings, and Future Plan for Implementation and Collaboration

Notable Outcomes: The primary outcome is a **fully functional, multi-layered prototype** that successfully demonstrates three critical security innovations: a working implementation of unphishable, certificate-bound tokens; a real-time 3ehavioural threat detection shield; and a successful end-to-end Zero-Knowledge Proof verification system.

Key Learnings: This hackathon has been an immense learning experience. I gained deep, practical knowledge in implementing advanced cryptographic protocols like mTLS and zk-SNARKs, moving them from theoretical concepts to tangible code. Furthermore, I learned the importance of a decoupled, microservices-based architecture for building resilient, high-performance systems, especially when dealing with mixed I/O-bound and CPU-bound workloads.

Future Plan for Implementation and Collaboration with Bank of Baroda: My vision is for Bank of Baroda to adopt this framework as a **core strategic asset**. We propose a phased implementation roadmap:

1. **Phase 1 (Foundation):** Pilot Layer 1 (Unphishable Identity) on the bank's most critical payment APIs to immediately eliminate the risk of credential theft.
2. **Phase 2 (Intelligence):** Activate and train the Layer 2 Proactive Shield on Bank of Baroda's unique API traffic to build an automated, intelligent defense system.
3. **Phase 3 (Innovation):** Launch a new, privacy-preserving digital product using Layer 3's Zero-Knowledge technology, such as instant income verification for lending partners, creating a unique market advantage.

Beyond internal defense, there is a powerful opportunity for Bank of Baroda to productize this technology as a **"BoB SecureConnect"** offering—providing Security-as-a-Service to its fintech partners. This would not only secure the entire ecosystem but also create a new, high-margin revenue stream.

6. Any Other Notable Point

This project is more than just a security solution; it's an enabler for the future of Digital India. By building a framework for secure and private financial data exchange, we create the trust necessary for the next generation of digital banking services to flourish. I am incredibly grateful for this opportunity and am eager to discuss how the "Intelligent API Security Fabric" can become a cornerstone of Bank of Baroda's digital future.

*****