Title: Revolutionizing Authentication for Payments: Secure, Efficient, and User-Centric Solutions

Overview:

In digital payments, secure authentication is critical to protecting user accounts and financial data. Traditional methods like passwords, SMS codes, and PINs are not only vulnerable to breaches but often create friction for users. The challenge here is to develop an innovative authentication solution that binds strongly to the user's identity while maintaining efficiency and ease of use.

Problem Statement:

Design and prototype a **next-generation authentication system** for payment platforms that establishes **a strong, reliable link between the user and their account**. The method should ensure security against common threats like phishing, social engineering, and replay attacks, while providing a seamless experience for users across different devices and environments.

Use Case:

1. **Retail Payment, Wholesale Payment, Business to Business Payment, It can be system agnostic solutions also.**

Key Objectives:

Participants should focus on designing authentication methods that achieve a robust connection between the user and their payment account. They are encouraged to explore or combine the following approaches, or propose their own solutions:

1. **Biometric Binding with Anti-Spoofing Measures**: Develop a system that uses biometric features (e.g., facial recognition or fingerprint) as the primary means of authentication. To enhance security, implement anti-spoofing technologies (e.g., liveness detection) to prevent fraudsters from bypassing the authentication using photos or 3D models. Consider how biometrics can securely link a user's face or fingerprint to their payment account across devices.
2. **Behavioral Biometrics for Continuous Authentication**: Incorporate behavioral biometrics, such as typing patterns, touchscreen interactions, or gait analysis, to maintain an ongoing authentication check. Continuous behavioral tracking can enhance

security by verifying that the legitimate user remains active throughout a transaction, adding an additional layer to prevent unauthorized access.

3. **Secure Device-Based Key Storage**: Use the secure elements of mobile devices (such as the hardware security module or trusted execution environment) to store cryptographic keys tied to a user's biometric profile. These keys should facilitate seamless, single-step authentication for payments and minimize exposure of sensitive data.
4. **Context-Aware Authentication**: Design an adaptive, context-aware authentication system that strengthens security based on contextual data like location, device fingerprint, or transaction history. For example, lower-risk transactions may require simpler authentication, while high-risk scenarios may demand stronger, multi-factor verification.
5. **Multi-Factor Authentication (MFA) Redesign**: Create a frictionless, innovative multi-factor approach that combines factors like biometrics, device proximity, or one-time keys, without relying on outdated methods like SMS. The solution should prioritize convenience and usability while ensuring robust security.
6. **Strong User-Account Binding Through Biometrics**: Ensure that your authentication approach strongly binds the user's biometric identity directly to their payment account. Explore how account data can be securely linked to the user's biometrics, allowing for re-authentication across multiple sessions and devices without weakening the security link.

Deliverables:

1. **Prototype**: A working prototype of your authentication solution that simulates a payment transaction.
2. **Technical Documentation**: Outline the authentication approach, security measures, and any cryptographic or hardware features utilized. Provide a security analysis highlighting how the solution protects against potential attack vectors.

3. **Performance and Usability Report**: Assess the efficiency and user-friendliness of the solution, particularly for mobile and low-power devices.
4. **Exploratory Report**: Discuss trade-offs made between security, efficiency, and user convenience, as well as the potential for real-world deployment.

Evaluation Criteria:

1. **Security**: How effectively does the solution prevent unauthorized access, including protection against biometric spoofing and other forms of fraud?
2. **Efficiency**: Is the authentication process quick and easy to use without compromising security? How well does it perform on low-resource devices?
3. **Usability**: Is the user experience smooth, intuitive, and convenient? Does it reduce friction while maintaining a high level of security?
4. **Innovation**: Originality in rethinking authentication methods with an emphasis on secure user-account binding.
5. **Robustness**: How well does the system handle different use cases, such as multi-device access, and does it maintain a strong user-account link?