✅

Specific and Sub Objectives

One specific objective for the development of a secure and context-aware multi-factor authentication (MFA) system for admin access using machine learning (ML) and biometric behavior analysis is to improve the accuracy and reliability of the authentication process while ensuring the system's resilience against attacks.

Sub-objectives to achieve this objective could include:

1. To develop an ML model that accurately and reliably identifies authorized admin users based on their biometric behavior patterns.
2. To integrate the ML model with a rule-based system that monitors the output of the ML model and detects any anomalies or inconsistencies.
3. To improve the resilience of the ML model against attacks using model robustness techniques, such as adversarial training.
4. To continuously monitor and update the ML model and the rule-based system to adapt to changing threats and attacks.
5. To evaluate the accuracy, reliability, and resilience of the MFA system through extensive testing and analysis, including testing under adversarial conditions.
6. To assess the usability and user experience of the MFA system and make any necessary improvements to ensure ease of use and adoption by admin users.
7. To develop clear and concise documentation for the MFA system, including user manuals, system specifications, and security guidelines, to ensure secure and efficient use of the system.

These sub-objectives would enable the development of a robust and effective MFA system that accurately and reliably identifies authorized admin users while being resilient to attacks and adaptable to changing threats. Additionally, ensuring that the MFA system is user-friendly and well-documented would enhance the overall usability and adoption of the system by admin users.