🌊

Methodology

1. Data Collection: The first step is to collect a comprehensive dataset of biometric behavior patterns from authorized admin users. This dataset should include a wide range of behaviors, such as typing rhythm, mouse movements, and mobile device usage.
2. Feature Extraction: Once the dataset is collected, the next step is to extract relevant features from the collected data. This step involves identifying and selecting features that are most relevant to the authentication process, such as keystroke duration, mouse movement speed, and device orientation.
3. Model Selection: The third step is to select an appropriate ML model for the MFA system. This step involves evaluating various ML algorithms, such as neural networks and support vector machines, and selecting the best model based on performance metrics such as accuracy, precision, and recall.
4. Model Training: The selected ML model is trained using the extracted features and the collected data from authorized admin users. This training process involves adjusting the model's parameters to optimize its performance and minimize errors.
5. Rule-Based System Integration: Once the ML model is trained, it is integrated with a rule-based system that monitors the output of the ML model and detects any anomalies or inconsistencies.
6. Model Robustness Improvement: To improve the resilience of the ML model against attacks, techniques such as adversarial training can be employed to train the model to detect and defend against adversarial attacks.
7. Testing and Evaluation: The MFA system is tested and evaluated using a variety of testing scenarios, including normal usage scenarios and adversarial attack scenarios. Performance metrics such as accuracy, false positive rate, and false negative rate are measured to assess the system's effectiveness.

8. Usability Assessment: The usability and user experience of the MFA system are evaluated through user surveys and interviews. The system's ease of use and user adoption are assessed, and any necessary improvements are made.
9. Documentation: Finally, comprehensive documentation is developed for the MFA system, including user manuals, system specifications, and security guidelines, to ensure secure and efficient use of the system.