PERFORMANCE AND FINAL SUBMISSION PHASE

MODEL PERFORMANCE METRICS

DATE	04 NOVEMBER 2023
TEAM ID	NM2023TMIDO2213
PROJECT NAME	BIOMETRIC SECURITY SYSTEM FOR VOTING PLATFORM
MAXIMUM MARK	4 MARKS

When assessing the performance of a biometric security system for a voting platform, it's essential to use appropriate metrics to evaluate its effectiveness and accuracy. Biometric security systems are designed to verify the identity of voters using unique physiological or behavioral characteristics. Here are some key performance metrics to consider:

1. False Acceptance Rate (FAR) or False Match Rate (FMR):
   - FAR measures the rate at which the system incorrectly accepts an unauthorized voter as a legitimate one. It is crucial to keep this rate as low as possible to prevent fraudulent voting.
2. False Rejection Rate (FRR) or False Non-Match Rate (FNMR):
   - FRR measures the rate at which the system incorrectly rejects a legitimate voter. A high FRR can disenfranchise voters, so it should be minimized.
3. Equal Error Rate (EER):
   - The EER is the point at which the FAR and FRR are equal. It is a crucial metric to determine the overall accuracy of the system. A lower EER indicates better performance.
4. Receiver Operating Characteristic (ROC) Curve:
   - The ROC curve is a graphical representation of the trade-off between FAR and FRR at different decision thresholds. A good system will have an ROC curve that hugs the upper-left corner, indicating high accuracy.
5. Genuine Acceptance Rate (GAR) or True Match Rate (TMR):

- GAR measures the rate at which the system correctly accepts authorized voters as legitimate. A high GAR is essential for a reliable biometric system.

6. Failure to Enroll Rate (FER):
   - FER quantifies the failure rate of the system when attempting to enroll a voter in the biometric database. A high FER can lead to difficulties in onboarding voters.
7. Template Matching Score:
   - For biometric systems that use templates for comparison, the template matching score can be analyzed to determine the degree of similarity between the biometric sample and the stored template.
8. Crossover Error Rate (CER):
   - CER is the point on the ROC curve where the FAR and FRR are equal. It is a useful summary metric for comparing different biometric systems.
9. Failure to Capture Rate:
   - This metric measures the rate at which the system fails to capture a biometric sample correctly. A high failure to capture rate can result in frustrated voters.
10. Throughput:
- Throughput measures how quickly the system can process voter verifications. A high-throughput system is essential for handling a large number of voters efficiently.

11. User Experience:
- Consider collecting user feedback on the ease of use and satisfaction with the biometric system. Positive user experiences are crucial for the adoption and success of the voting platform.

12. Security Against Spoofing:
- Evaluate the system's resistance to spoofing attempts (e.g., using fake fingerprints or facial images). Assess how well it can detect and prevent such attacks.

It's important to tailor the selection of metrics to the specific biometric modalities used in your system (e.g., fingerprint, iris, face recognition, voice recognition). Additionally, the legal and ethical considerations surrounding biometric voting systems should be taken into account to ensure privacy and security.

Regular testing and monitoring of these metrics will help maintain the integrity of the voting platform and ensure that the biometric security system performs effectively.

Is this conversation helpful so far?