Adversarial-AI CAPTCHA Solver for Accessibility

1. Motivation & Goals

Blind or motor-impaired users often hit dead-ends on sites protected by CAPTCHAs. Our goal is to build an ethical, robust service that:

- ***Automatically solves** text, image and audio CAPTCHAs*
- ***Integrates** seamlessly with screen-readers and form-fillers*
- ***Maintains privacy** by not persisting challenge data*
- ***Monitors** solver performance and adapts to new CAPTCHA schemes*

---

*2. **Components***

- ***Client Extension***
    - *Chrome/Firefox plugin + iOS/Android SDK*
    - *Captures CAPTCHA payload → sends to Preprocessing API*
    - *Receives solution → auto-enters or exposes to assistive tech*
- ***Preprocessing API***
    - ***Text CAPTCHAs:** Grayscale, threshold, deskew*
    - ***Image CAPTCHAs:** Segment into character blobs via U-Net*
    - ***Audio CAPTCHAs:** Band-pass filter, noise reduction*
- ***Solver Service***
    - *Hybrid CNN/Transformer ensemble in PyTorch*

    - *Adversarial module (FGSM/PGD) to perturb inputs for maximum clarity*
    - *Multi‑stage pipeline:*
        1. *Baseline recognition*
        2. *Adversarial refinement*
        3. *Final prediction*
- ***Confidence Estimator***
    - *Returns a probability score*
    - ***≥ 0.8:** Auto‑submit; **< 0.8:** route to Fallback UI*
- ***Fallback UI***
    - *Simplified view with high‑contrast image/audio player*
    - *Screen‑reader–friendly prompts for manual override*
- ***Logging & Retraining***
    - *MongoDB logs: challenge hash, timestamps, solution, confidence*
    - *Daily job: cluster low‑confidence failures → fine‑tune model*
    - *Versioned artifacts stored in S3*

---

*3. **Admin Dashboard** (React + D3)*

- *Upload new challenge samples*
- *Monitor solve‑rate, latency, error clusters*
- *Configure retraining schedule (cron/airflow)*
- *Manage holiday/blacklist for abusive domains*

---

4. Security & Privacy

- ***Ephemeral Processing:** Challenges held in memory only*

- ***TLS Everywhere:*** *Extension ↔ API ↔ Solver*
- ***Access Control:*** *OAuth2 for admin; token-based for clients*

---

5. Scalability & Deployment

- ***Kubernetes*** *autoscaling for solver pods*
- ***RabbitMQ*** *queue for high-volume bursts*
- ***Prometheus + Grafana*** *for real-time metrics*

---

6. Deliverables

- *Client extension packages (Chrome, Firefox, iOS, Android)*
- *Containerized Preprocessor & Solver with Helm charts*
- *Training pipeline (Docker + Airflow DAGs)*
- *React-based Admin UI*
- *Full documentation: setup, scaling, security*

---

7. Impact & Ethics

- *Grants equal web access, meeting WCAG & ADA*
- *Continuous feedback loop prevents bias toward any CAPTCHA vendor*
- *Transparent logs support audits without exposing PII*

Ready for deep technical Q&A on adversarial attacks, model ensembles, and secure integrations.