CodHer'25
Anna University, Chennai.

BRO CODE

AI POWERED SELF HEALING SECURITY FOR CONNECTED VEHICLES

GEN AI IN SECURITY

START

OUR TEAM: BRO CODE

TEAM MEMBERS

ABHI LAVANYA

KRISHNENDU M R

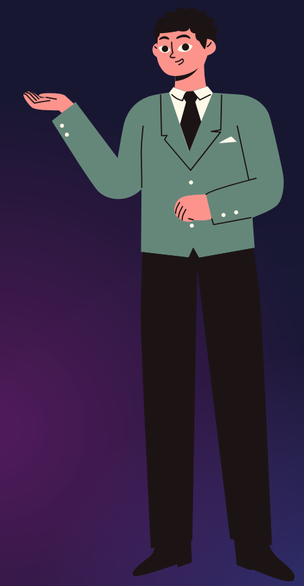
SARASHIVASRI S

Why would anyone hack a car? I mean... cars aren't like computers, right?

Not anymore. Modern cars are basically rolling computers!!! They have internet access, they stream music, get live traffic, and park themselves. And if it's connected, it can be hacked...

If cars are connected, they need protection.
That's why we built FleetGuard — the self-healing AI shield for connected vehicles.

NEXT



NEED FOR INTELLIGENT CYBERSECURITY IN CONNECTED VEHICLES

Increasing cyber threats targeting in-vehicle networks (e.g., CAN bus).

Traditional IDS lacks real-time, autonomous mitigation.

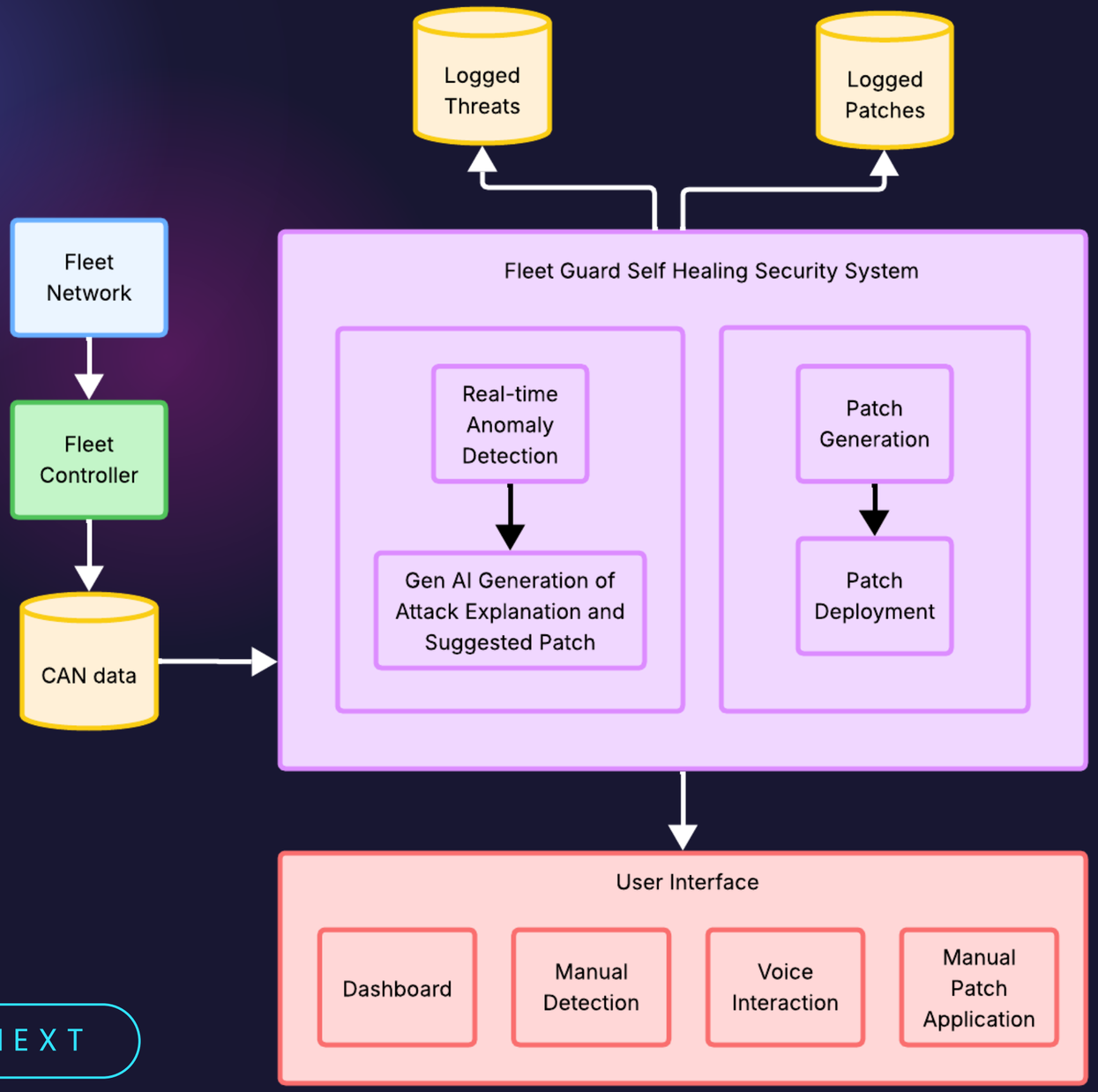
Attackers can remotely cut brakes or steer, risking lives and system safety.

Need for AI-powered system that detects and heals attacks automatically.

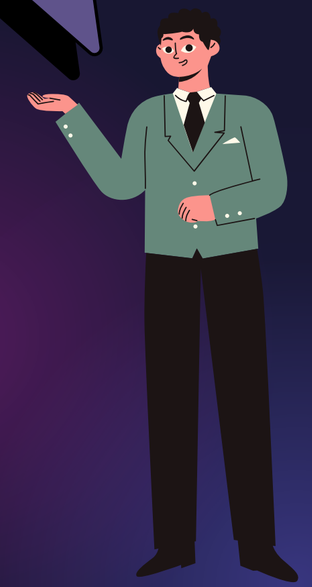
Goal: Provide self-healing security for smart, connected vehicles.

NEXT

SYSTEM ARCHITECTURE DIAGRAM



CAN data is the real-time language cars use to talk — like speed, braking, or engine status. A patch is a quick software fix we send to stop an attack or fix a bug, just like updates on your phone.



NEXT

AI POWERED SELF-HEALING SECURITY SYSTEM

Generates real-time vehicle data to mimic driving behavior.

Isolation Forest/ Random Forest identifies abnormal patterns.

SpeechRecognition Transcribes audio commands; TTS gives audible response.

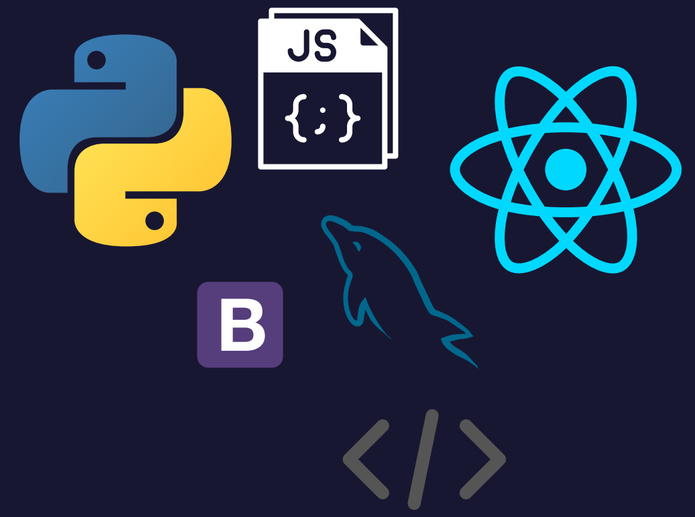
Stores attack history with GPT explanation, suggested patch and prediction results.

Suggests and sends patch over the air to mitigate detected threats.

Provides human-like explanations for anomalies.

NEXT

TECHNICAL STACK



1. **Frontend:** React.js, JavaScript, REST API, React Bootstrap
2. **Backend:** Python, Flask, SQLite, Threading
3. **Machine Learning:** Scikit-learn (IsolationForest, RandomForestClassifier)
4. **Natural Language Processing(NLP):** Hugging Face Transformers-GPT2LMHeadModel, GPT2TokenizerFast, Trainer, TrainingArguments, DataCollatorForLanguageModeling
5. **Voice Interface:** SpeechRecognition, pyttsx3

NEXT

CHALLENGES AND SOLUTIONS

CAN Data Interpretation: Fine-tuned GPT-2 for human-readable threat explanations

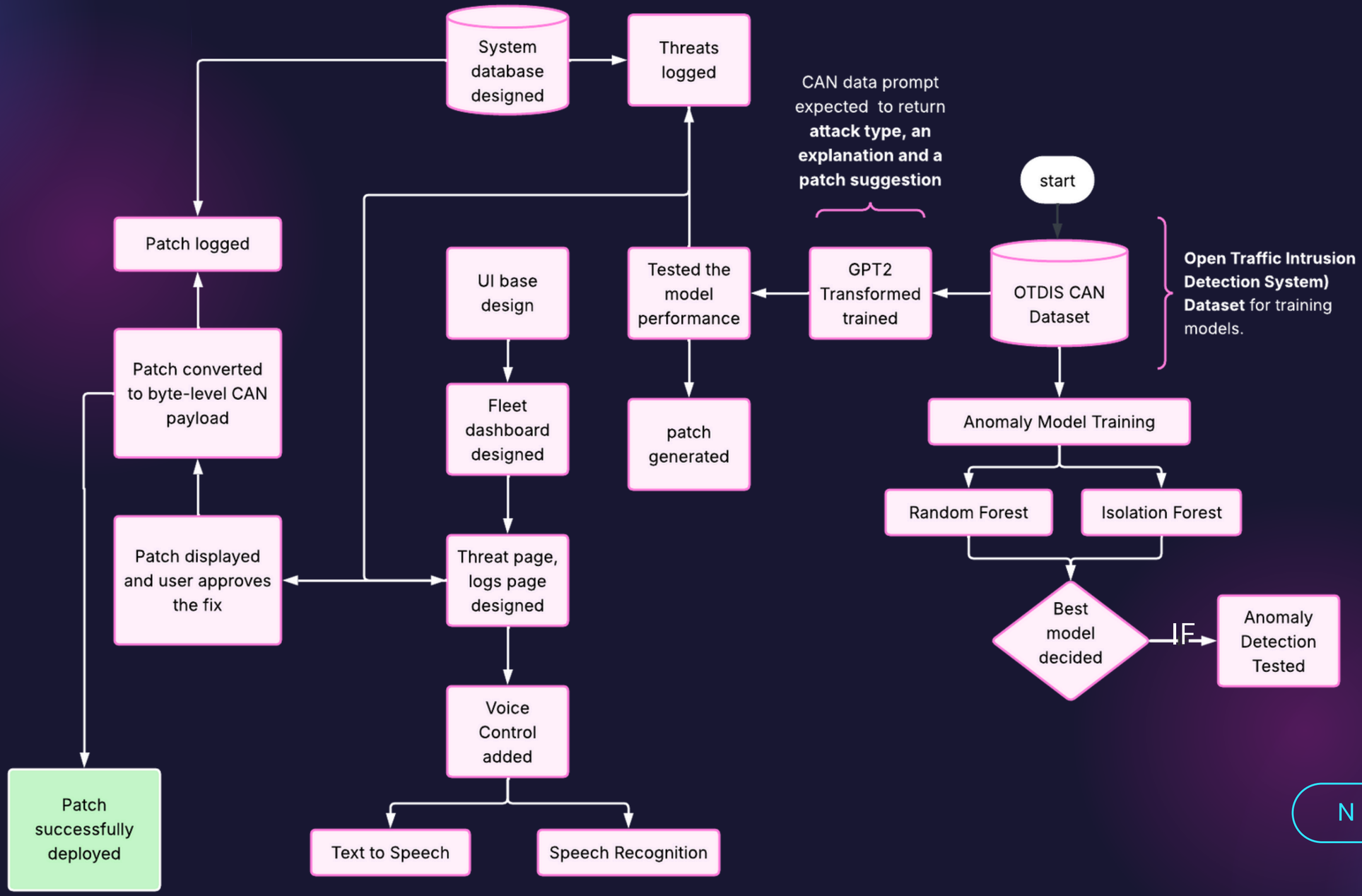
Real-Time Patching: Built a self-healing loop for instant detection and patch deployment

Model Selection: Tested models on OTDIS; chose Isolation Forest for best accuracy

User Accessibility: Added dashboard, voice interface, and AI logs for non-tech users

NEXT

IMPLEMENTATION DETAILS



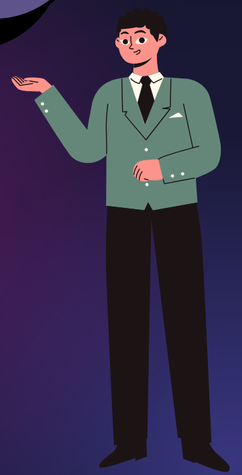
NEXT

CONCLUSION AND FUTURE SCOPE

So far.....

- Developed a self-healing real-time AI module for detecting and patching cyberattacks in connected vehicles.
- Fine-tuned DistilGPT-2 on CAN data to generate attack type, explanation, and patch suggestions.
- Added support for speech-based interactions

Future scope includes larger LLMs for smarter detection, launch a mobile app, test on a real vehicle, and enable real over-the-air (OTA) patch updates.



THANKYOU