David Gibb

Asabre Ebenezer

Project 3: Home safety using LLM agents

Explain how the team is suitable for the project

David Gibb:

Programming experience:

* 5 years professional experience
  + 2 years as project lead
* B.S. in computer engineering
* 2 years using python

Relevant Courses Taken:

* ECE 601 Machine Learning
* ECE 629 Applied Machine Learning for IoT
* ECE 603 Statistics
* ECE 633 Advanced stochastic process theory

Currently watching:

* Deep Learning playlist overview
* Langchain tutorials
* machine learning intro

others:

Asabre Ebenezer:

Programming experience: Python, C, Java, Embedded Prog, Web Design

Relevant Courses Taken: W3schools Machine learning, w3 schools data science

Currently watching: Functions, Tools and Agents with LangChain, Deep Learning playlist overview & machine learning intro

Due to the above experiences that we bring onboard, our team is suitable for taking on this project.

MOTIVATION

Home security is a major concern for modern homeowners, but traditional security systems often result in high rates of false alarms or require real-time monitoring. By leveraging Large Language Models (LLMs), we aim to create a more intelligent and user-friendly solution where users upload security images, and the system generates a textual description of the image to detect any suspicious behavior. This approach reduces the complexity of live data monitoring and provides accurate, actionable insights to enhance home security.

DESIGN GOALS

### **Project Goal:**

* To develop a system that analyzes uploaded images from home security cameras using an LLM-powered captioning model, generating descriptions of the scenes and flagging any suspicious activities or potential intruders.

### **Specific Goals:**

1. **Image Captioning**: Accurately describe objects, people, and movements in an image using an image captioning model.
2. **Intruder Detection**: Analyze captions through an LLM to determine whether any descriptions suggest suspicious or unusual behavior.
3. **User Interface**: Create a simple, user-friendly web interface where users can upload security images and receive alerts or reports on potential intrusions.
4. **Scalability**: Ensure the system can easily integrate with existing security setups, allowing users to manually upload security images.

### **Deliverables:**

* **LLM Agent Understanding**: Complete tutorials on LLM agents and frameworks like Langchain.
* **Agent Setup**: Implement basic LLM agents based on the provided tutorials.
* **Home Safety System**: Develop the LLM-powered home safety system with threat detection (e.g., intruder).
* **Code Generation**: The LLM should output code snippets for key safety tasks, such as object detection door locking algorithms.
* **System Documentation**: Comprehensive documentation, including tutorials and walkthroughs.
* **Demonstration Video**: A video showcasing the system in action.

#### **System Blocks**

* **Data Input**: Sensors such as camera to gather environmental data.
* **LLM Reasoning**: A pre-trained LLM agent equipped with tools for analyzing data from images.
* **Action Output**: Depending on the LLM's reasoning, the system will trigger actions like activating alarms, locking doors, or generating code for safety protocols.
* **User Interface**: A dashboard where users can monitor and configure system settings.

#### **Hardware/Software Requirements**

* **Hardware**:
  + Laptop with CUDA-enabled GPU (or use Google Colab)
  + Sensors: Cameras for intruder detection
  + Microcontroller for sensor integration (optional)
* **Software**:
  + Python for integrating the LLM
  + Langchain or other agent frameworks
  + Google Colab for training if a GPU is not locally available
  + API for sensor data input and action triggers

#### **Team Member Responsibilities**

* **Setup and Networking**: David – Colleague. Responsible for setting up the basic LLM integration using tutorials.
* **Software**: Asabre – User. Responsible for writing and integrating the software components, including LLM configuration, reasoning setup, and action-trigger mechanisms.
* **Writing**: Asabre & David –. Responsible for writing documentation, deliverables, and project reports.
* **Research**: David – Colleague. Focused on researching the best LLM tools, configurations, and possible improvements.
* **Algorithm Design**: Asabre – User. Designing and implementing algorithms for threat detection and response mechanisms.

#### **References**

* Langchain tutorial:<https://www.deeplearning.ai/short-courses/functions-tools-agents-langchain/>
* Paper on LLM agents:<https://arxiv.org/pdf/2303.17580>
* Fire detection datasets and object detection models for training.