**Capstone Project Details:**

**Development of an AIML Tool for Phishing Domain Detection**

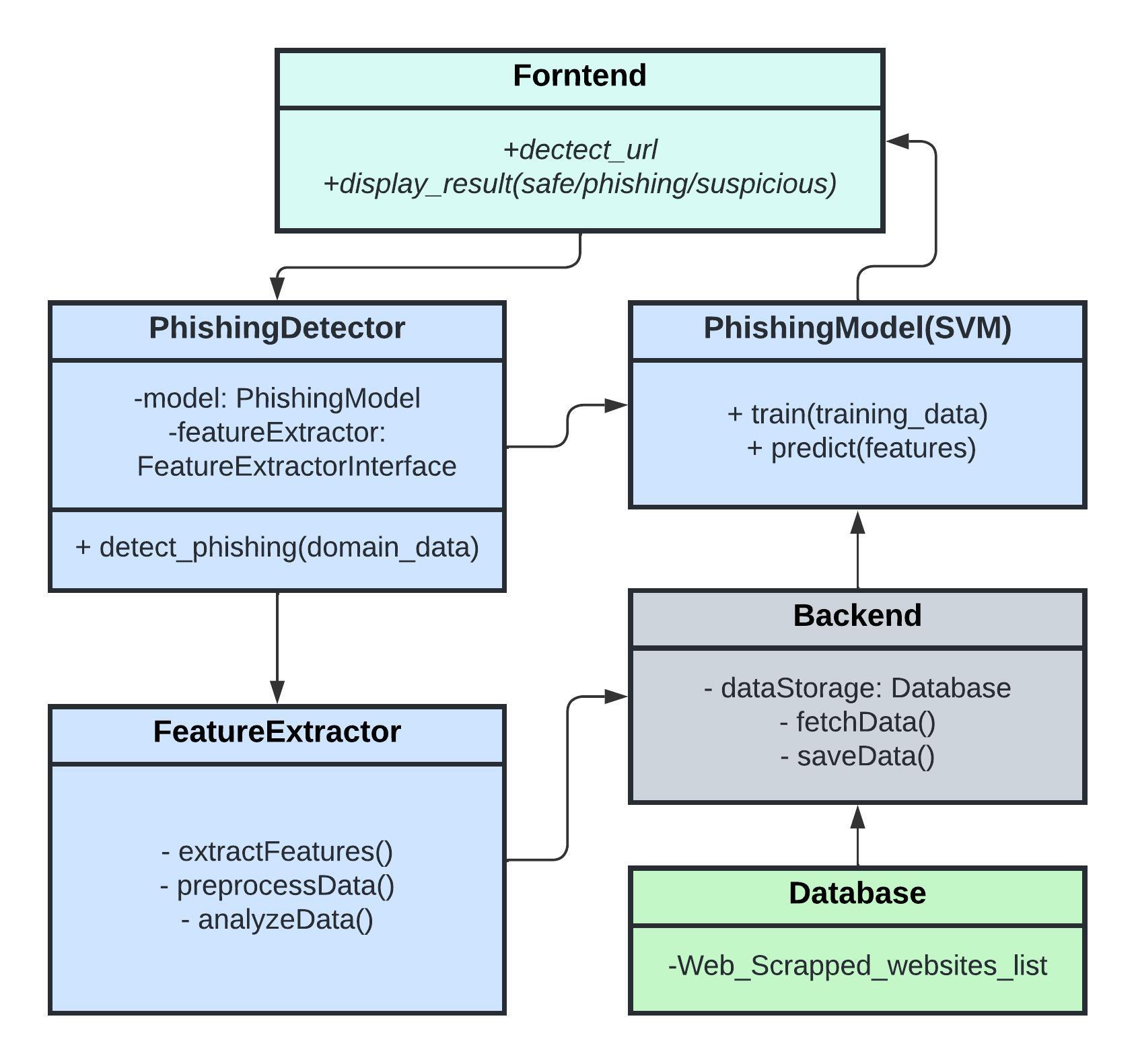
1. **Introduction:**

This capstone project focuses on developing an Artificial Intelligence and Machine Learning (AIML) tool to accurately identify phishing domains. Phishing remains a prevalent cybersecurity threat, and the tool aims to utilize advanced algorithms and methodologies to mitigate risks posed by fraudulent websites.

1. **Technology Description:**
   1. **AI and ML Algorithms:** The tool will utilize supervised learning algorithms like Random Forest, Support Vector Machines (SVM), and neural networks for precise domain classification.
   2. **Natural Language Processing (NLP):** Employing NLP techniques, the tool will extract and analyze textual features from domain URLs to enhance detection accuracy.
   3. **Data Preprocessing Techniques:** Various preprocessing methods will be applied to clean and prepare the dataset, ensuring optimal performance during model training.
   4. **Web Scraping:** Data collection from online sources will be facilitated.
2. **Hardware Device Details:**

The tool is designed to operate on standard computing hardware with adequate processing power and memory capacity.

1. **Software Product Information:**
   1. **Operating System:** Compatibility with major operating systems such as Linux and Windows will ensure widespread accessibility.
   2. **Development Tools:** Python will be the primary programming language, supported by essential libraries including TensorFlow, and Scikit-learn.
   3. **Database:** Data storage and management will be handled efficiently using robust systems like Excel.
2. **Programming Languages:**
   1. Python will serve as the primary language due to its versatility and ease of development.
   2. Additional libraries and frameworks like TensorFlow, Scikit-learn, and NLTK will augment the tool's capabilities in machine learning and natural language processing.
3. **System Component Descriptions:**
   1. **Data Collection**: The tool will efficiently gather domain data from diverse online sources and repositories.
   2. **Feature Extraction:** NLP techniques will extract relevant features from domain URLs to facilitate accurate classification.
   3. **Model Training:** Rigorous training of machine learning models using preprocessed data will ensure robust performance.
   4. **Inference:** Trained models will be deployed for real-time classification of domain URLs, enhancing cybersecurity measures.
4. **Component Diagrams and Design Requirements:**



1. **Construction or Fabrication Details:**

While primarily a software project, comprehensive instructions will be provided for any physical device construction if necessary for deployment. (Under the Instruction\_to\_run…. file)

1. **Conclusion:**

The development of an AIML tool for phishing domain detection is crucial for combating cybersecurity threats effectively. Through the integration of advanced algorithms and technologies, this project endeavours to create a robust solution that safeguards users against phishing attacks. The outcomes of this capstone project have the potential to significantly bolster cybersecurity measures and protect the interests of online users.