Group 3 Main Project Topics

Gautham C Sudheer
(U2103092)

Fathima Jennath
(U2103089)

Godwin Gino
(U2103096)

Mohammed Basil
(U2103139)

1. Enhanced Malayalam Parser for Dataset Creation

The “Malayalam Parser for Dataset Creation” project aims to address the scarcity of annotated datasets in the Malayalam language for Natural Language Processing (NLP) applications. The primary objective is to develop a robust Malayalam parser capable of analyzing the syntactic and semantic structures of Malayalam sentences. This parser will not only serve as a fundamental tool for linguistic analysis but also aim to develop educational tools and explore other possible applications with the dataset created. The creation of this parser involves several key steps, including data collection from diverse sources, preprocessing to ensure data quality, and manual annotation of a representative subset of the data with grammatical and syntactic information. The parser development process encompasses the selection of an appropriate parsing approach, whether rule-based, statistical, or machine learning-based. The model is trained using the annotated Malayalam dataset, focusing on capturing the unique linguistic nuances of the Malayalam language. Evaluation metrics are employed to assess the parser’s performance on a separate test set, guiding iterative refinement and enhancement.

The resulting Malayalam parser serves as a valuable tool for the analysis of grammatical structures in new Malayalam text data, contributing to the creation of high-quality Malayalam datasets crucial for advancing NLP research and applications in the Malayalam language. This project encourages collaboration with linguists, researchers, and the Malayalam-speaking community to ensure linguistic accuracy and relevance in the development of the parser. By developing educational tools, the project aims to facilitate language learning and teaching, providing resources for both students and educators. Furthermore, the annotated dataset created by the parser can be utilized in various applications such as machine translation, speech recognition, and sentiment analysis, expanding the scope and impact of Malayalam NLP. The ”Malayalam Parser for Dataset Creation” project aligns with the broader goal of promoting linguistic diversity in NLP, addressing the challenges posed by the scarcity of resources for underrepresented languages. Through the development of this parser, the project aims to facilitate further research and innovation in Malayalam NLP, opening avenues for the exploration of various language-related tasks and applications.

2. Phishing Detection Browser Extension

Phishing attacks represent an escalating threat in the digital realm, targeting users with deceptive emails, counterfeit websites, and fraudulent forms to steal sensitive information. Traditional security measures, such as static blocklists and periodic scans, fall short against these rapidly evolving threats. This project aims to develop a solution that detects and mitigates phishing attempts in real-time by leveraging advanced techniques like behavior-based analysis and machine learning, analyzing web content and user interactions as they happen to prevent data breaches and financial losses effectively.

The primary objective is to implement real-time detection of phishing attempts using a combination of browser extension frameworks and machine learning. By analyzing URLs and domains, the system evaluates their reputation against known phishing threats, providing a robust layer of security. The solution employs content analysis to scan web pages and email content for indicators of phishing. Key tools include Chrome Extension API/WebExtensions API for development, TensorFlow.js for deploying machine learning models directly in the browser, and crypto-js for securing data. Additionally, external servers (Flask/Django) handle complex machine learning models, while APIs like VirusTotal and Google Safe Browsing assess URL reputations.

The project will deliver a fully operational browser extension compatible with major browsers like Chrome, Firefox, and Edge, offering real-time phishing detection. Users will receive immediate notifications and detailed warnings about detected phishing attempts, along with recommended actions to avoid them. By providing immediate protection against phishing attempts, this solution will enhance user confidence in digital interactions and promote safer online practices. Ultimately, the project aims to foster cybersecurity awareness and set a new standard for phishing protection, contributing to the broader effort of combating cyber threats in the digital age.

3. Intrusion Detection System

Traditional Intrusion Detection Systems (IDS) face significant challenges in keeping up with the rapid evolution of cyber threats, making it difficult to detect unknown or zero-day attacks. There is a critical need for an adaptive and effective IDS capable of identifying and mitigating both known and unknown security breaches in real-time. The proposed solution leverages machine learning (ML) algorithms to enhance the capabilities of IDS, providing a more robust defense against cyber threats. By incorporating Local Interpretable Model-agnostic Explanations (LIME), the system offers transparency and interpretability of model predictions, allowing for a deeper understanding of the detection process and improving trust in the system's decisions.

The primary objective of this project is to develop an adaptive and interpretable IDS using ML. Specific objectives include collecting and preprocessing network traffic data, extracting relevant features for training ML models, training ML models to classify network traffic as normal or malicious, and using LIME to explain the decisions made by the models. Tools such as Wireshark and Tcpdump for data collection, Scikit-learn, TensorFlow, and Keras for feature extraction and training, and LIME for interpretability will be employed. Standard metrics like Accuracy, Precision, Recall, and F1-Score will assess model performance, ensuring rigorous evaluation of the IDS to guarantee its effectiveness.

The project aims to achieve high detection rates for both known and unknown attacks, with minimal false positives. The IDS will provide clear, understandable explanations for model predictions using LIME, ensuring transparency and trustworthiness. The end product will be a robust and interpretable IDS that enhances cybersecurity measures, strengthening the overall resilience of networks against cyber threats. This innovative system will contribute to a safer digital environment, benefiting both individuals and organizations by protecting sensitive information and fostering trust in digital infrastructures.