Anomaly Detection

Internal Guide:
Mrs. Divyani Tirthyani

Priyansh Tailor

(IU2141051155)

ABSTRACT/INTRODUCTION

This project focuses on developing a machine learning (ML) based Anomaly Detection system tailored for User and Entity Behavior Analytics (UEBA). By integrating ML algorithms into a user-friendly web interface, this system enables organizations to identify irregular patterns and potential security threats through user behavior data analysis. The application allows users to select and configure various ML processes such as data cleaning, formatting, feature scaling, and feature selection, followed by the application of selected ML models to detect anomalies effectively.

OBJECTIVE

The primary objective of this project is to enhance security measures within organizational IT frameworks by automatically detecting anomalous user activities, such as repeated login failures, which could indicate potential security threats or breaches. The system aims to provide a dynamic and configurable approach to data analysis, ensuring adaptability to various use cases within the realm of UEBA.

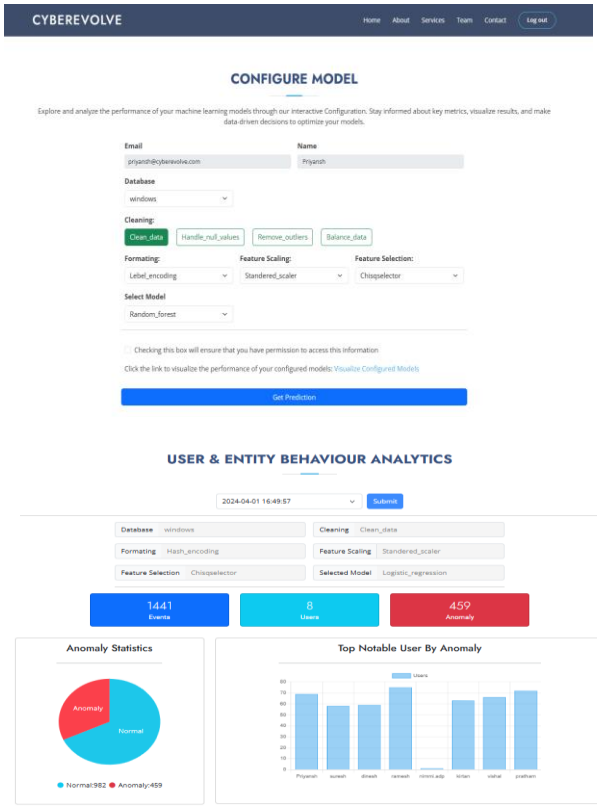
TOOLS AND TECHNOLOGY

- Frontend: Developed using HTML, CSS, Bootstrap, and JavaScript to create an interactive and easy-to-navigate interface.
- Backend: MySQL, Python, specifically utilizing Flask as a web framework for handling web server requests and serving the ML model's output.
- Machine Learning: Python libraries such as Scikit-learn for implementing ML algorithms, and PySpark for data manipulation.
- Visualization: JavaScript libraries like Chart.js for presenting data visualizations that depict anomalies and patterns within the user data.

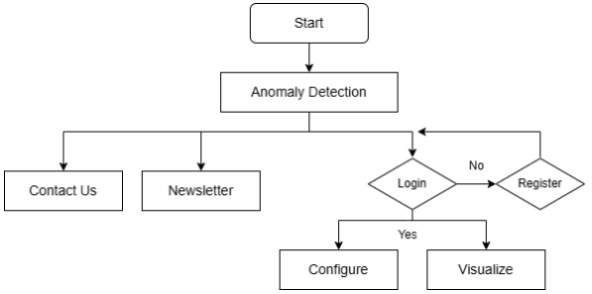
SOCIAL BENEFITS

This anomaly detection system significantly improves security monitoring within organizations by proactively identifying and responding to unusual activities that could precede security incidents. It empowers security analysts by providing tools that augment their capabilities to predict, detect, and mitigate potentially harmful actions based on user behavior data, thus protecting sensitive information and infrastructure.

SCREENSHOTS



FLOWCHART



FUTURE ENHANCEMENT

Future enhancements will focus on expanding the range of detectable anomalies by incorporating more sophisticated ML models and integrating more comprehensive user behavior datasets to cover a broader spectrum of potential security threats. Further development will also aim at improving real-time data processing capabilities to enable instant anomaly detection and response.

CONCLUSION

The Anomaly Detection project represents a crucial step forward in applying machine learning to enhance organizational security. By automating the detection of unusual user behaviors, the system not only improves security responsiveness but also enables organizations to safeguard their digital environments more effectively. As cyber threats evolve, so too will the capabilities of systems like these, continually adapting to new challenges in the field of cybersecurity.