Robust CyberSecurity Threat Detection Systems

A PROJECT REPORT

Submitted by

AARYAN MAHESHWARI	**22BDO10001**
CHAYAN GOPE	**22BDO10036**

in partial fulfillment for the award of the degree of

Bachelors of Engineering

IN

Computer Science with specialization in DevOps.

Chandigarh University

August 2024

CONTENT

INTRODUCTION

1. DESCRIPTION OF OUR PROPOSAL::

   This project aims to develop a robust cybersecurity threat detection system that leverages machine learning and advanced analytics to identify, classify, and respond to potential security threats in real time. The system will focus on detecting various types of threats, including malware, phishing attempts, network intrusions, and other cyberattacks.

2. OBJECTIVES OF OUR PROPOSAL::

   - To Develop a comprehensive threat detection framework using machine learning algorithms.
   - To Implement real-time monitoring and alerting mechanisms for detecting and responding to cyber threats.
   - To ensure the system can classify different types of threats accurately.
   - To Integrate the system with existing network infrastructure and security tools.
   - To Conduct extensive testing to evaluate the system's effectiveness and robustness.

3. TOOLS & TECHNOLOGIES USED IN OUR PROJECT::

- **Programming Languages:** Python (for machine learning models), JavaScript (for front-end and real-time data visualization), Bash (for scripting).

- **Frameworks/Libraries:** TensorFlow or PyTorch (for ML model development), Scikit-learn (for data preprocessing and modeling), ReactJS (for front-end).

- **Databases:** MySQL/ (for storing logs and threat data), ElasticSearch (for real-time data indexing and searching).

- **Tools:** Jupyter Notebook (for data analysis and model development).

- **Cloud Services:** AWS(for scalable infrastructure and deployment, future scope)

4. SCOPE OF OUR PROPOSAL::

The scope of the Robust Cybersecurity Threat Detection System project encompasses the development of a system that can detect, classify, and respond to various cyber threats in real time. The project will focus on utilizing machine learning to analyze network traffic, system logs, and other data sources to identify potential threats, such as malware, phishing, and network intrusions. The system will include automated incident response capabilities, allowing it to take immediate action when a threat is detected. Additionally, the project will integrate with existing security tools and be designed for scalability, enabling deployment in cloud and on-premises environments. However, the project will not cover advanced threat-hunting techniques or the development of new encryption methods.

5. CONCLUSION::

In conclusion, the Robust Cybersecurity Threat Detection System is designed to address the growing challenges of modern cybersecurity threats by leveraging advanced machine learning techniques and real-time monitoring capabilities. This project aims to enhance the security posture of organizations by accurately detecting and classifying threats, automating incident response, and seamlessly integrating with existing security tools. The system's scalability ensures its adaptability to various environments, making it a valuable asset in safeguarding digital infrastructures. Upon completion, this project will not only provide a robust defense against evolving cyber threats but also contribute to creating a safer and more resilient digital landscape.

6. TEAM ROLES::

Name	UID	Roles
Aaryan Maheshwari	22BDO10001	TEAM LEAD
Chayan Gope	22BDO10036	MEMBER

Supervisor's Signature   Student's Signature

Mamta Sharma (E15565)