**DIAGNOSIS INTELLIGENCE**

A report submitted in partial fulfillment of the requirements for the Degree of

## Bachelor of Technology

In

## Computer Science and Engineering (Cyber Security)

by

V.Teja 2111CS040136

Under the esteemed guidance of

Mrs.Affrose

## Assistant Professor



**Department of Computer Science & Engineering (Cyber Security) School of Engineering**

**MALLA REDDY UNIVERSITY**

## Maisammaguda, Dulapally, Hyderabad, Telangana 500100

**2024**

**DIAGNOSIS INTELLIGENCE**

A report submitted in partial fulfillment of the requirements for the Degree of

## Bachelor of Technology

In

## Computer Science and Engineering (Cyber Security)

by

V.Teja 2111CS040136

Under the esteemed guidance of

**Mrs. Affrose**

**Assistant Professor**



## Department of Computer Science & Engineering (Cyber Security) School of Engineering

**MALLA REDDY UNIVERSITY**

Maisammaguda, Dulapally, Hyderabad, Telangana 500100

## 2024



Department of Computer Science & Engineering (Cyber Security)

**CERTIFICATE**

This is to certify that the project report entitled “**Diagnosis Intelligence**”, submitted by

**V.Teja (2111CS040136)** towards the partial fulfillment for the award of **Bachelor’s Degree**

**in Cyber Security from the Department of Computer Science and Engineering, Malla Reddy**

**University,** Hyderabad, is a record of Bonafide work done by him/ her. The results embodied

in the work are not submitted to any other University or Institute for the award of any degree

or diploma.

### Internal Guide Head of the Department

Mrs. Affrose Dr. G. Anand Kumar

Assistant Professor CSE (Cyber Security & IoT)

### External Examiner

**DECLARATION**

We hereby declare that the project report entitled **“Diagnosis Intelligence”** has been carried out by us and this work has been submitted to the **Department of Computer Science and Engineering (Cyber Security), Malla Reddy University, Hyderabad** in partial fulfillment of the requirements for the award of degree of Bachelor of Technology. We further declare that this project work has not been submitted in full or part for the award of any other degree in any other educational institutions.

Place: Date:

|  |  |
| --- | --- |
| V.TEJA | 2111CS040136 |

**ACKNOWLEDGEMENT**

We extend our sincere gratitude to all those who have contributed to the completion of this project report. Firstly, we would like to extend our gratitude to **Dr. V. S. K Reddy, Vice-Chancellor**, for his visionary leadership and unwavering commitment to academic excellence.

We would also like to express our deepest appreciation to our project guide

**Mrs. Affrose** whose invaluable guidance, insightful feedback, and unwavering support have been instrumental throughout this project for successful outcomes.

We extend our gratitude to our **PRC convenor**, **Dr. G. Latha**, for giving valuable inputs and timely guidelines to improve the quality of our project through a critical review process. We thank our project coordinator, **Mrs. T. Suneetha**, for her timely support.

We are also grateful to our **Dr. G. Anand Kumar, Head of the Department of Cyber Security & IOT** for providing us with the necessary resources and facilities to carry out this project.

We thank **Dr. Harikrishna Kamatham**, **Dean, School of Engineering**, for his encouragement and support throughout my academic pursuit.

We are deeply indebted to all of them for their support, encouragement, and guidance, without which this project would not have been possible.

|  |  |
| --- | --- |
| V.TEJA | 2111CS040136 |

**ABSTRACT**

In the ever-evolving landscape of cybersecurity, traditional firewalls often struggle to keep pace with sophisticated and dynamically changing cyber threats. With the exponential increase in network traffic and attack complexity, conventional rule-based security mechanisms fail to provide real-time, adaptive protection. Malicious actors continuously devise new attack vectors, making it imperative for cybersecurity systems to integrate intelligent, data-driven methodologies for threat detection and prevention. Machine Learning (ML)-based firewalls have emerged as a promising solution to enhance network security by identifying anomalies, detecting malicious activities, and adapting to evolving cyber threats. The UNSW\_NB15 dataset, a comprehensive collection of real-world network traffic, presents an ideal benchmark for training robust ML models that can discern between normal and malicious activities.

To address these challenges, this study develops an ML-powered firewall integrating multiple machine-learning models, including Random Forest (95%), Extra Trees (94.85%), Decision Tree (93.69%), Multi-Layer Perceptron (MLP) (93.44%), Gradient Boosting (93.15%), K-Nearest Neighbors (KNN) (92.91%), and Logistic Regression (91.07%). Among these, Long Short-Term Memory (LSTM) networks achieved the highest accuracy, with a training accuracy of 96.665% and testing accuracy of 96.435%, demonstrating superior performance in adaptive threat detection. The system is deployed using a user-friendly Streamlit-based UI, enabling real-time threat detection by allowing users to upload CSV files containing network traffic data. The firewall not only identifies potential threats but also provides preventive measures based on detected anomalies, offering a proactive approach to network security.