Intrusion Detection System(IDS)

**Submitted for**

**Artificial Intelligence and Machine Learning CSET301**

Submitted by:

(E23CSEU1558) Nischay Khurana

Submitted to:

Jan–May 2025

**DR. Yajnaseni Dash**

**Jan-May 2025**

**SCHOOL OF COMPUTER SCIENCE AND ENGINEERING**

A close-up of a logo

Description automatically generated

**INDEX**

|  |  |  |
| --- | --- | --- |
| Sr.No | Content | Page No |
| 1 | Abstract | 3 |
| 2 | Introduction | 3 |
| 3 | Related Work | 3 |
| 4 | Methodology | 4 |
| 5 | software | 4 |
| 6 | results | 4 |
| 7 | conclusion | 5 |
| 8 | Future scope | 5 |
| 9 | Github Link | 6 |
| 10 | Reference | 6 |

# Abstract

This project presents an Intrusion Detection System (IDS) using Deep Learning techniques. It utilizes an Autoencoder for anomaly detection and a Convolutional Neural Network (CNN) for attack classification. Using the NSL-KDD dataset, the system can detect and classify various types of network intrusions with high accuracy.

# Introduction

With the increasing growth of digital networks, securing them from malicious attacks is crucial. Traditional systems often fail to adapt to new and evolving threats. Deep learning models, especially Autoencoders and CNNs, offer a data-driven solution for identifying both known and unknown attack patterns.

# Related Work

Many IDS systems have utilized shallow machine learning algorithms like Decision Trees and SVMs. Recent advancements in Deep Learning have made it possible to handle large-scale and high-dimensional data more effectively, thus improving intrusion detection accuracy.

# Methodology

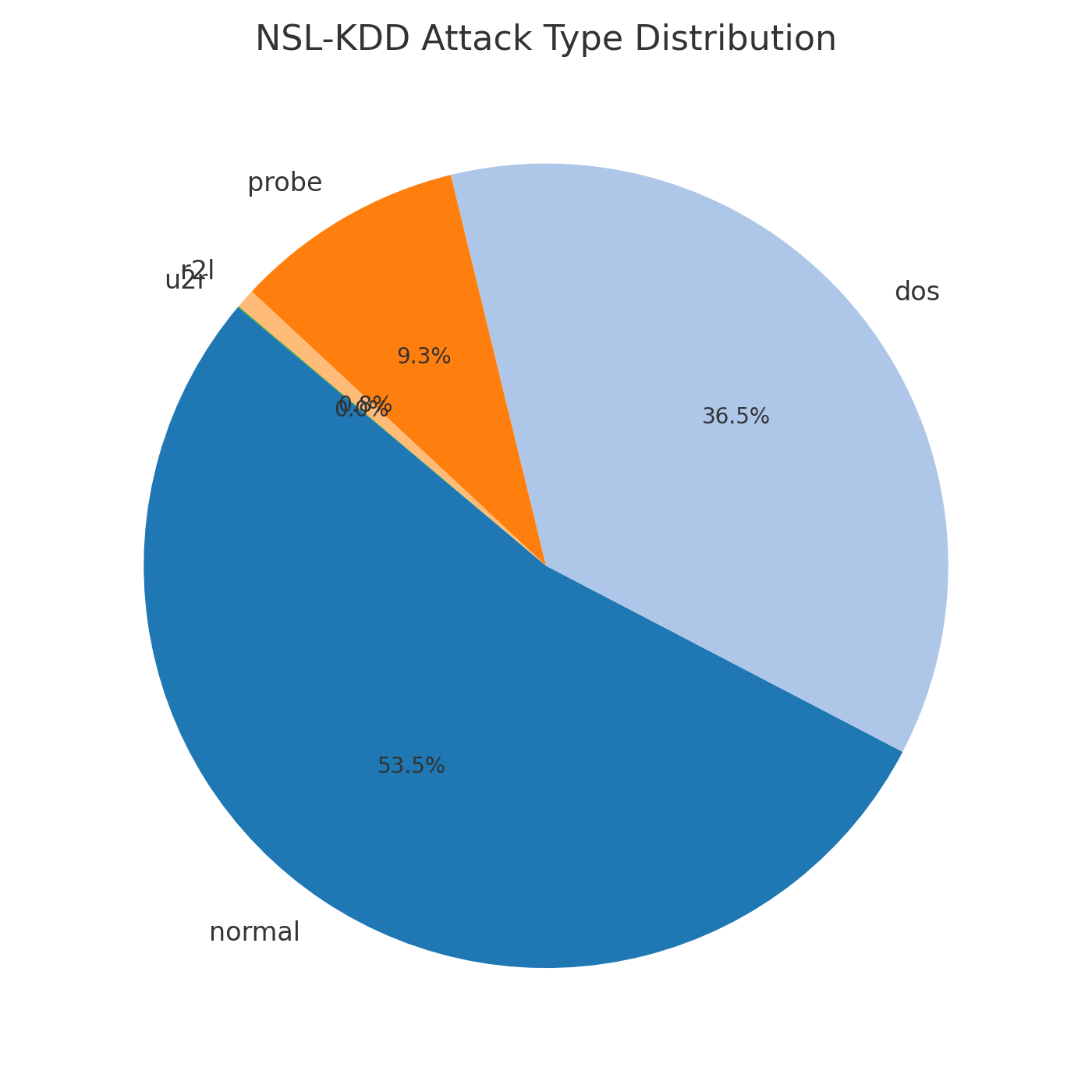
The system uses two main components:  
- Autoencoder: Trained on normal data to learn network behavior. Reconstruction error is used to detect anomalies.  
- CNN: Used for multiclass classification of network attacks using labeled NSL-KDD data.  
The dataset is preprocessed with normalization and label encoding. Models are trained using Keras/TensorFlow.

# Software Required

- Python 3.x  
- Flask  
- TensorFlow / Keras  
- Pandas / Numpy / Matplotlib  
- Render/Vercel for deployment

# Experimental Results

The models were evaluated using NSL-KDD dataset. Below is a chart showing the distribution of attack types.



The Autoencoder effectively detected anomalous traffic with high reconstruction error. The CNN classifier accurately classified attacks such as DoS, Probe, R2L, and U2R with significant performance. Accuracy for CNN classification was around 98%.

# Conclusions

This project demonstrates how deep learning can be used to build an effective IDS. By combining Autoencoder and CNN models, the system is capable of both anomaly detection and attack classification.

# Future Scope

- Integrate real-time packet capturing tools  
- Deploy on cloud for scalability  
- Extend dataset to include recent threats  
- Implement ensemble models for further accuracy improvements

# GitHub Link

https://github.com/nischay-1558/Intrusion-Detection-System

# References

https://youtu.be/wUMObYAhQ4I?feature=shared

# Project Screenshots

