

MINOR PROJECT REVIEW



# SMART INTRUSION DETECTION SYSTEM



# Contents

**INTRODUCTION**  
**OUR SYSTEM**  
**TECHNOLOGIES USED**  
**APPLICATIONS**  
**CONCLUSION**



# INTRODUCTION

An intrusion detection system (IDS) is a device or software programme that watches for hostile activity or policy breaches on a network. They are used to detect anomalies in order to catch hackers before they cause serious network or device harm.

When it detects potentially harmful packets or threats on Internet Protocol (IP) networks, it monitors traffic in real time and logs in alerts for users.



# Smart Intrusion Detection System

Our Intrusion Detection System focuses on developing a unique application, with the aid of Snort, which takes into consideration the user comfort, and makes the traffic and threats easier to detect, analyze and mitigate with the help of a dashboard.


The dashboard contains various unique features:

- Statistics about the weekly reports resolved, Alerts pending for review, and the critical alerts.
- A Pie Chart showcasing the different types of Packets received by the system.
- An Alert Graph showcasing the Resolved, In Progress and Pending Alerts.

As soon as any malicious activity is detected, an alert is logged in real-time.



# Technologies Used

- MongoDB for the database
  - React and Nodejs for the front-end and back-end
  - Snort IDS in Ubuntu for rules and traffic monitoring
  - Kali Linux for testing, generating suspicious traffic
- 



# Real Life Applications

Any IDS, no matter how efficient, requires human intervention in most cases before taking action as there is a high ratio of false positives and with that, the issue that arises is sometimes, IDS are too complex to understand or run on a system for users.

Our system aims at increasing the usability and understandability of the working of an IDS by developing a dashboard for analysing the data easily and notifying the user for malicious activities.

# THANK YOU

Presented by:

18BCE056

18BCE064