Intrusion Detection on KDD Dataset

GROUP 20
Divya Chaganti
Saili Sahasrabuddhe
Ashwin Viswanathan
Vignesh Miriyala
Sanil Sinai Borkar

KDD Dataset

- **Features**

  protocol_type: *symbolic*, src_bytes: *continuous*, wrong_fragment: *continuous*, hot: *continuous*, root_shell: *continuous*, su_attempted: *continuous*, num_access_files: *continuous*, srv_serror_rate: continuous, rerror_rate: *continuous*, diff_srv_rate: *continuous*

- **Types of Attacks**: buffer_overflow, ftp_write, guess_passwd etc.
- **Link to the dataset** - *http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html*

Problem Definition

- **Feature extraction** - Planning to use PCA to identify relevant features.
- **Classification** - Identifying a given data packet is malicious or benign.
- **Association** - Rules governing type of attack on RHS and identify other strong associations
- **Clustering** - Expected number of clusters equal to the different types of attacks

THANK YOU