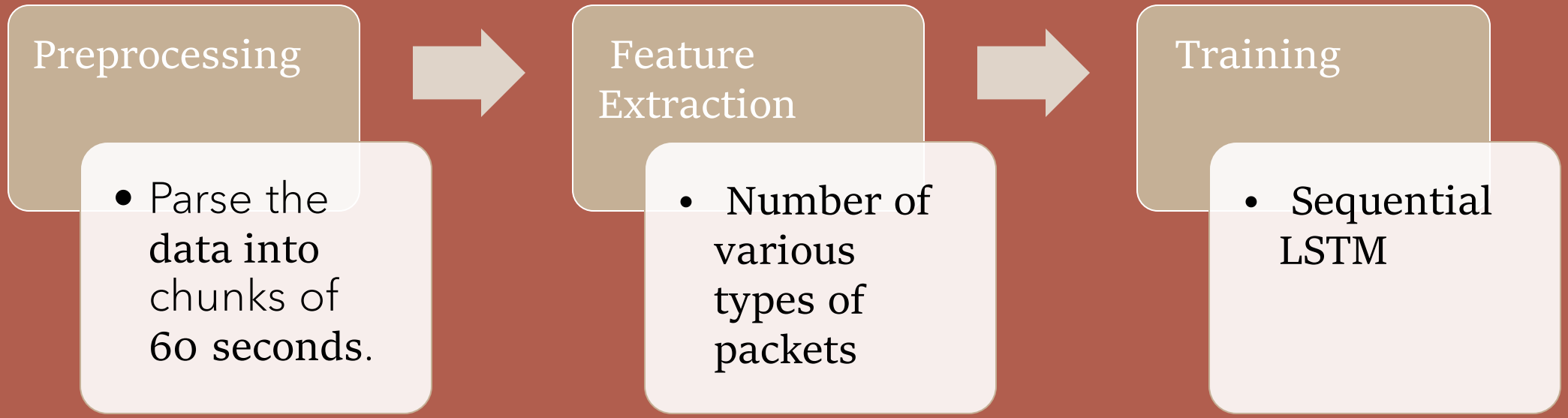
Hawk Eyes

DDOS Attack Detection

Outline

- Model the problem as classification of time series data.

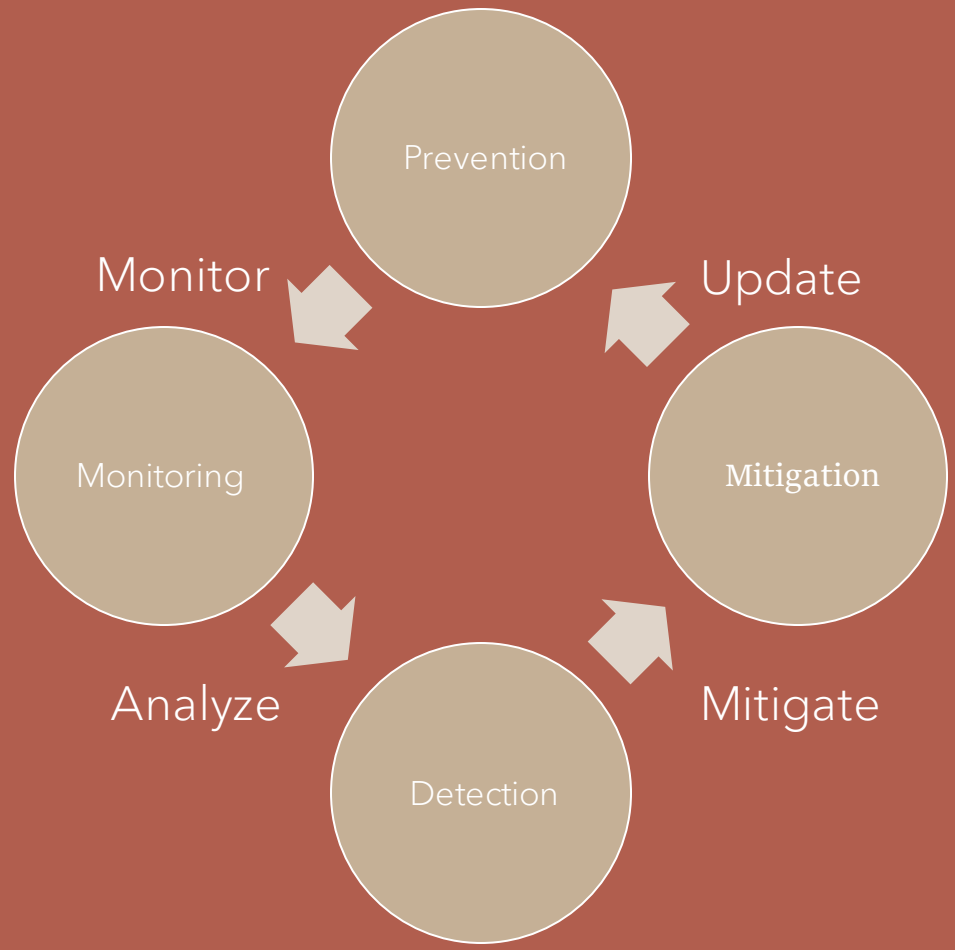


Salient Features

- Lightweight solution.
  - Low computation cost
- Best in class accuracy on provided dataset.
- Near real-time detection.
- Raw data is used for detection.

Future Work

- We can further extend the project to make a complete tool which can work on real time data.
- We can further classify the type of DDOS attack.



Appendix

Training methodology:

- First, the data is converted into per second traffic flow in the network. The following
- fields were taken for analysis in the nth second :
    - Total packets.
    - Total TCP packets.
    - Total UDP packets.
    - Total ICMP packets.
    - Total number of TCP (SYN) packets.
    - Total number of TCP (SYN-ACK) packets.
- Now we have time-series data which demonstrates the flow of network traffic.
- The next step is to break the file into chunks of 60 seconds and each chunk is labeled same as file i.e. benign or malicious.
- Now we use LSTM model to train on the dataset.
- We have a sequential model with two LSTM layers and one dense layer.

Appendix

- Testing methodology:
  - During the time of testing the same pre-processing step, as in training is done. Now, even if one chunk of 60 seconds is predicted as Malicious then the whole file is labeled as malicious.
- Results:
  - We achieved 100% accuracy on the testing dataset. The spit was 75-25 between training and testing datasets.
  - Total number of files used in testing = 15(benign) + 22(malicious)