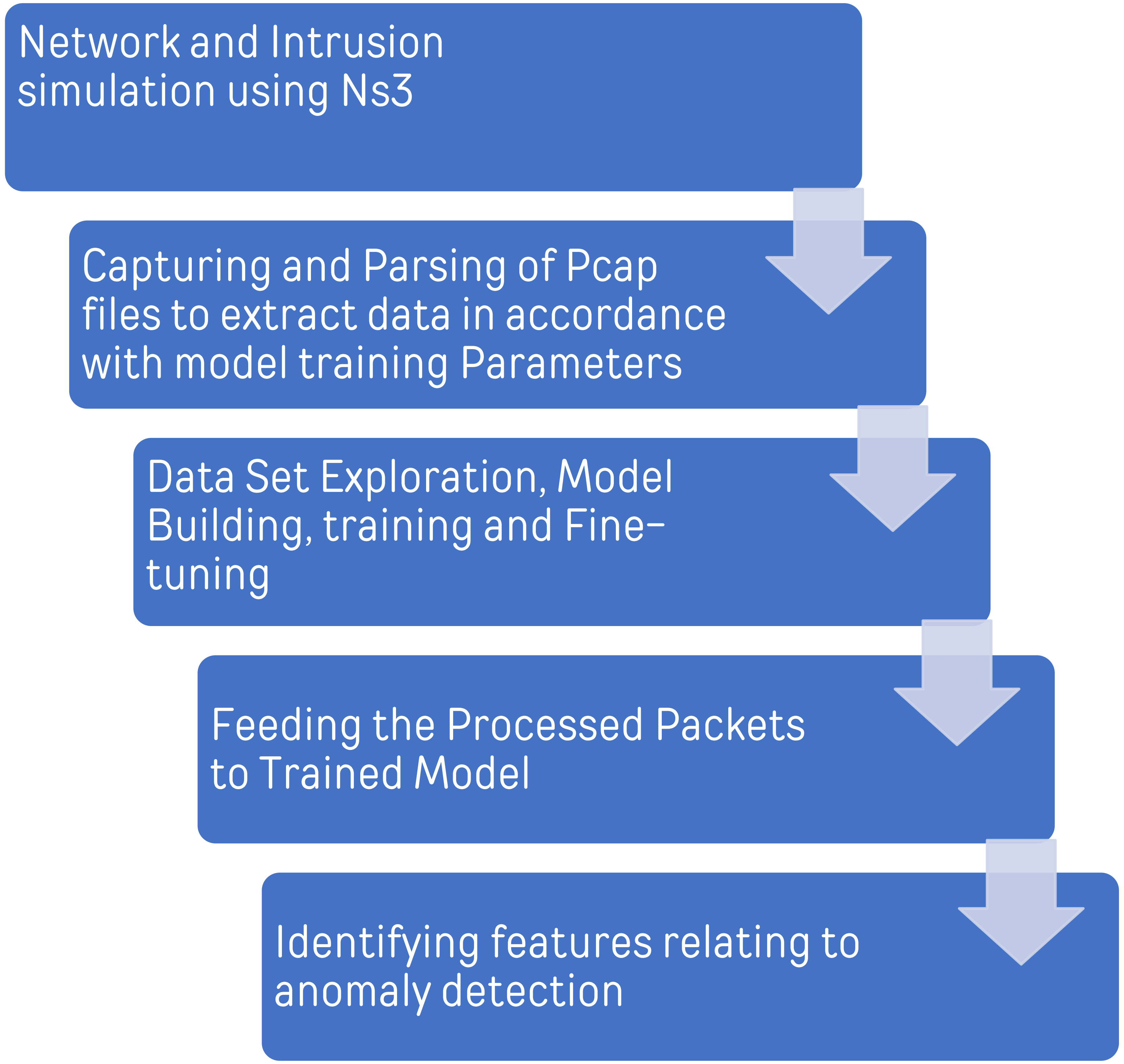
CN Project: Network Intrusion Detection System

- **ES21BTECH11003**
  - Aditya Bacharwar
- **ES21BTECH11006**
  - Aman Bhasin
- **ES21BTECH11007**
  - Ananya Varshney
- **ES21BTECH11022**
  - Avaneesh R Naik
- **ES21BTECH11024**
  - Abhinav Purli
- **ES21BTECH11028**
  - Saurabhkumar

Introduction to Network Intrusion Detection

- Network Intrusion Detection Systems (NIDS) are security mechanisms designed to monitor, detect, and respond to unauthorised or malicious activities within a computer network.
- The primary purpose is to enhance the security posture of a network by identifying and mitigating potential threats and intrusions.
- Provides continuous network traffic monitoring, allowing for real-time identification of anomalies and potential security breaches.
- Network Intrusion Detection Systems are critical components in modern cybersecurity, actively contributing to the proactive defence and resilience of computer networks. Their importance lies in their ability to detect and respond to potential threats, thereby ensuring the overall security of the network.

Project Overview



Network and Intrusion simulation using Ns3

Capturing and Parsing of Pcap files to extract data in accordance with model training Parameters

Data Set Exploration, Model Building, training and Fine-tuning

Feeding the Processed Packets to Trained Model

Identifying features relating to anomaly detection

Simulations Using NS 3

Distributed Denial of Service (DDoS) Simulation:

- DDoS attacks aim to overwhelm a target system or network by flooding it with overwhelming traffic from multiple sources, rendering the service unavailable to legitimate users.

NS3 Simulation Approach:

- **Traffic Generation**: Simulating numerous bot nodes to generate a high traffic volume towards a targeted node in t network area.
- **Bulk Send Helper:** The BulkSendHelper class in NS3 helped us simulate the heavy traffic using UDP packets.
- **Node Coordination:** Coordinating multiple nodes to simultaneously flood the target, mimicking the coordinated nature of real-world DDoS attacks.

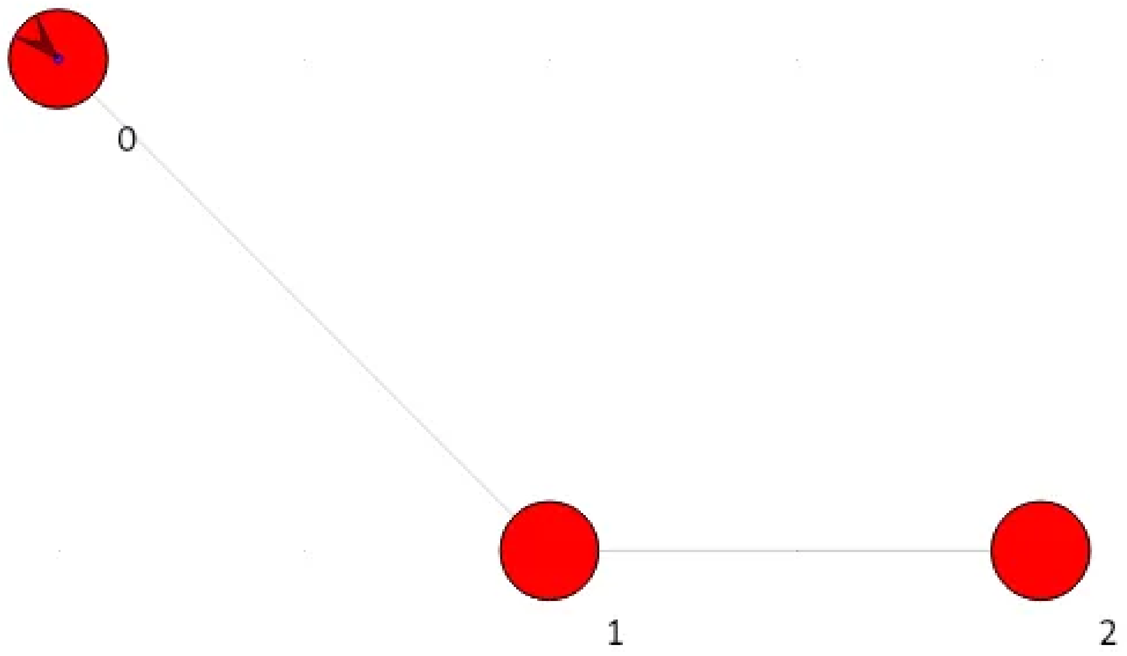
User to Root Attack (U2R) Simulation:

- U2R attacks involve an unauthorised user gaining elevated privileges within a system, often through exploiting vulnerabilities to escalate from a normal user to a system administrator or root-level access.

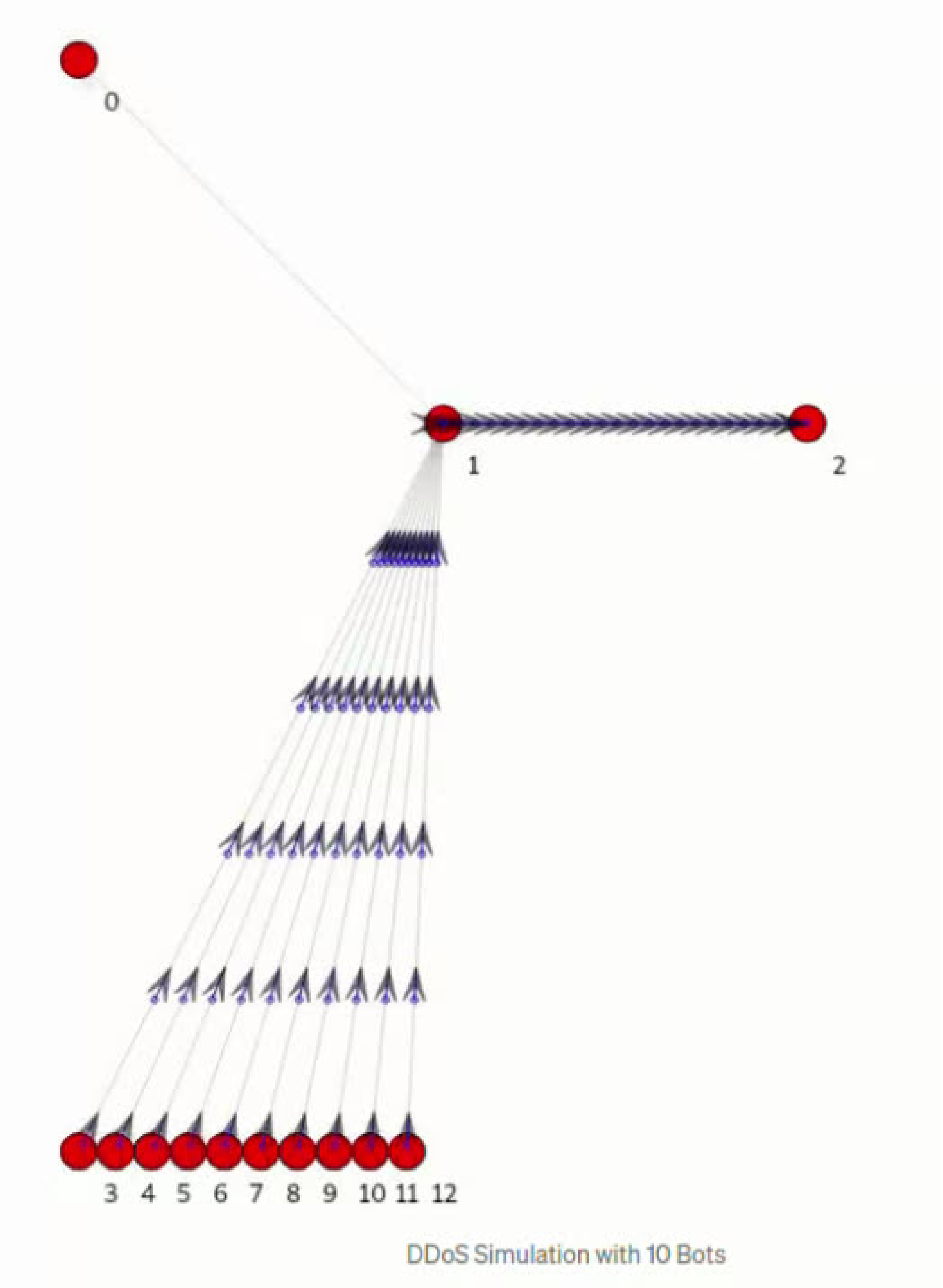
NS3 Simulation Approach:

- **Echo Server Setup:** An Echo Server is established on a node, listening on the given port. This server is created using the UdpEchoServerHelper class.
- **Malicious Traffic Generation:** The OnTime attribute is set to a constant random variable with a constant value of 1 second, indicating that the malicious traffic is generated for 1 second.
- **Pcap Traces for Analysis:** Pcap traces are enabled to capture network activity during the simulation. The traces are stored in files with the prefix "U2R" for further analysis.

Visualization of DDos Attack using NetAnim



Legitimate Network Connection



Multiple bot connections to simulate DDos Attack

Reading Features from PCAP Files

- Utilizing Wireshark, a powerful packet analysis tool, we gained various insights into packet attributes and structures, Such as source and destination IP addresses, ports, protocols, and flags, contributing to a comprehensive understanding of network traffic.
- Employed PyShark, a Python wrapper for Tshark (Wireshark's command-line counterpart), for capturing packets from PCAP files. It Enabled real-time packet capture, providing dynamic data for feature extraction.
- Developed scripts to parse captured packets, extracting relevant attributes critical for Intrusion Detection System (IDS) analysis. Extracted features like protocol type, source and destination addresses, service, ports, and flag information for detailed analysis.

Machine Learning Approach for NIDS

- Purpose:
    - Utilizing machine learning algorithms to enhance network security by identifying anomalous behaviour and potential threats within network traffic.
- Advantages:
    - ML enables NIDS to adapt, learn from new data, and improve detection accuracy over time.
- Strengthening Network Security:
    - Machine learning in NIDS enhances security by dynamically identifying both known and unknown threats within network traffic, surpassing the limitations of rule-based systems.
- Adaptive Learning Abilities:
    - ML equips NIDS with adaptive capabilities, allowing it to learn from diverse network data, update its detection mechanisms, and recognise emerging attack patterns.
- Continuous Learning from New Data:
    - ML-based NIDS continuously learns from incoming data, refining its models to improve detection accuracy over time, thereby staying current with evolving threats.
- Improved Accuracy and Proactive Detection:
    - Through iterative analysis, ML-driven NIDS sharpens its ability to discern anomalies, minimising false positives and proactively identifying potential threats to maintain network security.

Feature Selection for Model

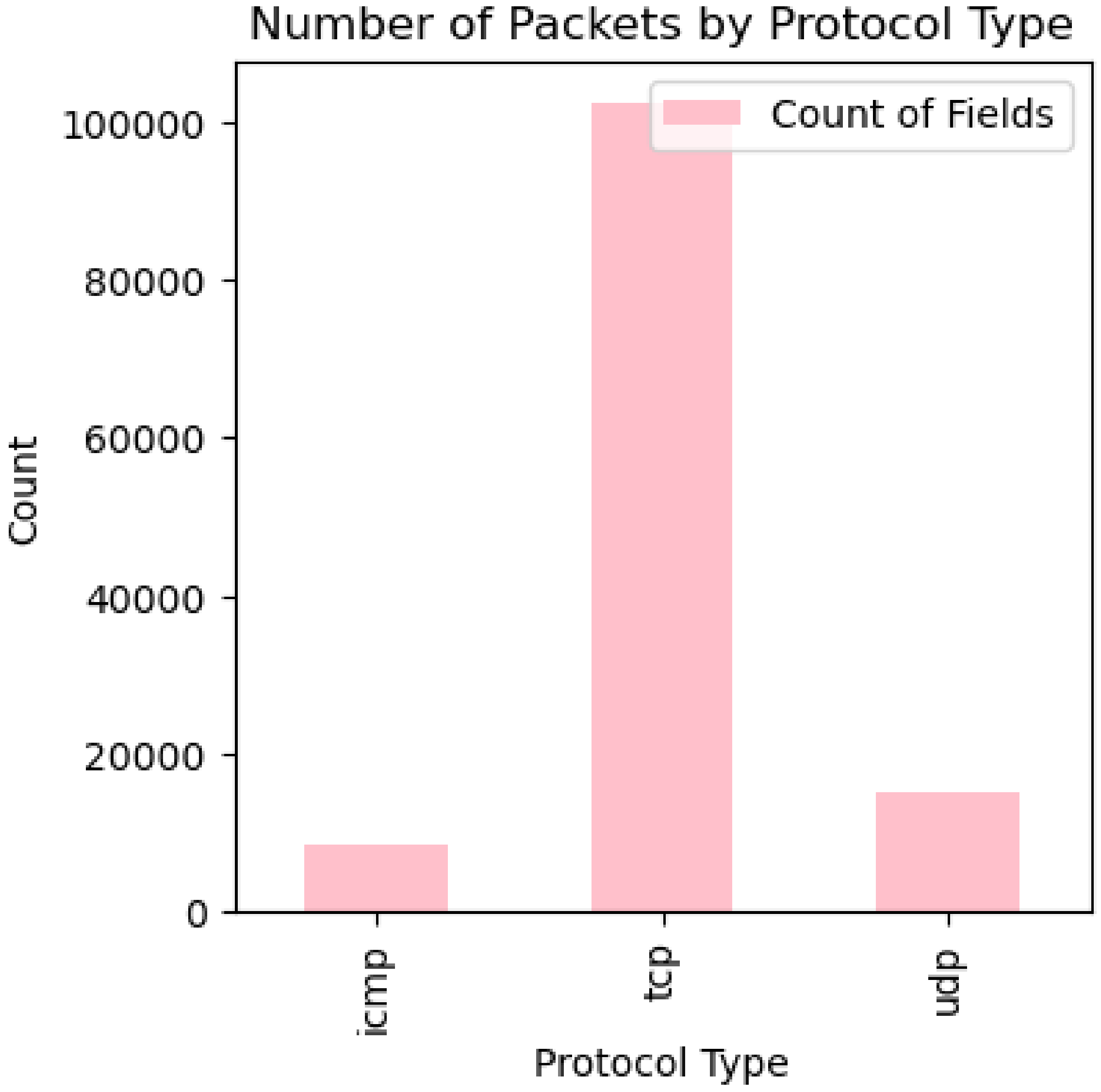
- We captured pcaps of the network and ran it through a feature extractor file
- Feature extractor file preprocessed the pcap and extracted the features
- The extractor file compressed the packets to (client-host) pair
- Each row in the output of the extractor file represents the Client-Host pair
- Each client-host pair had numerous features relevant to their connection
- Various protocol fields were used to extract the packets information

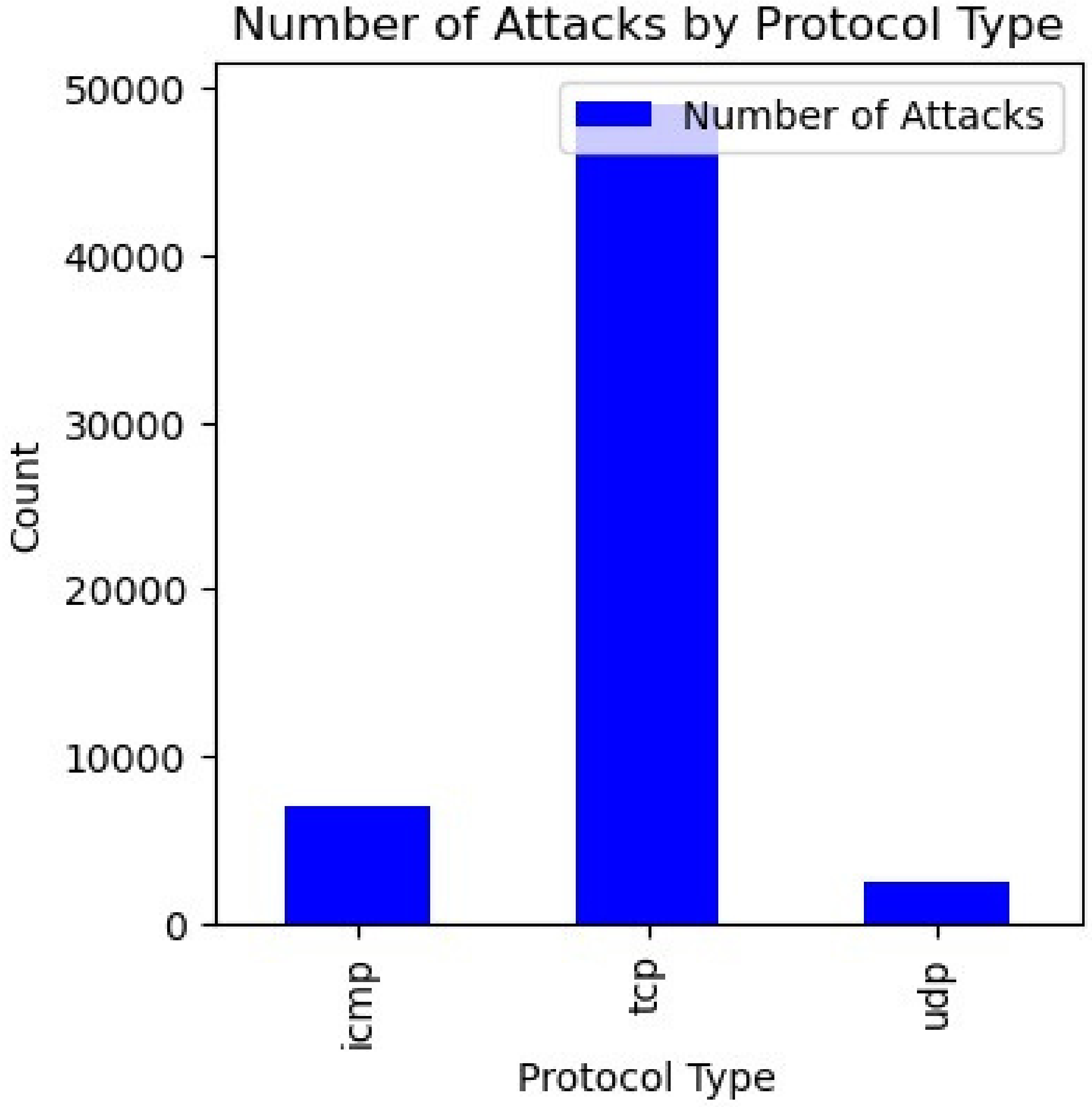
Model Architecture for Intrusion Detection

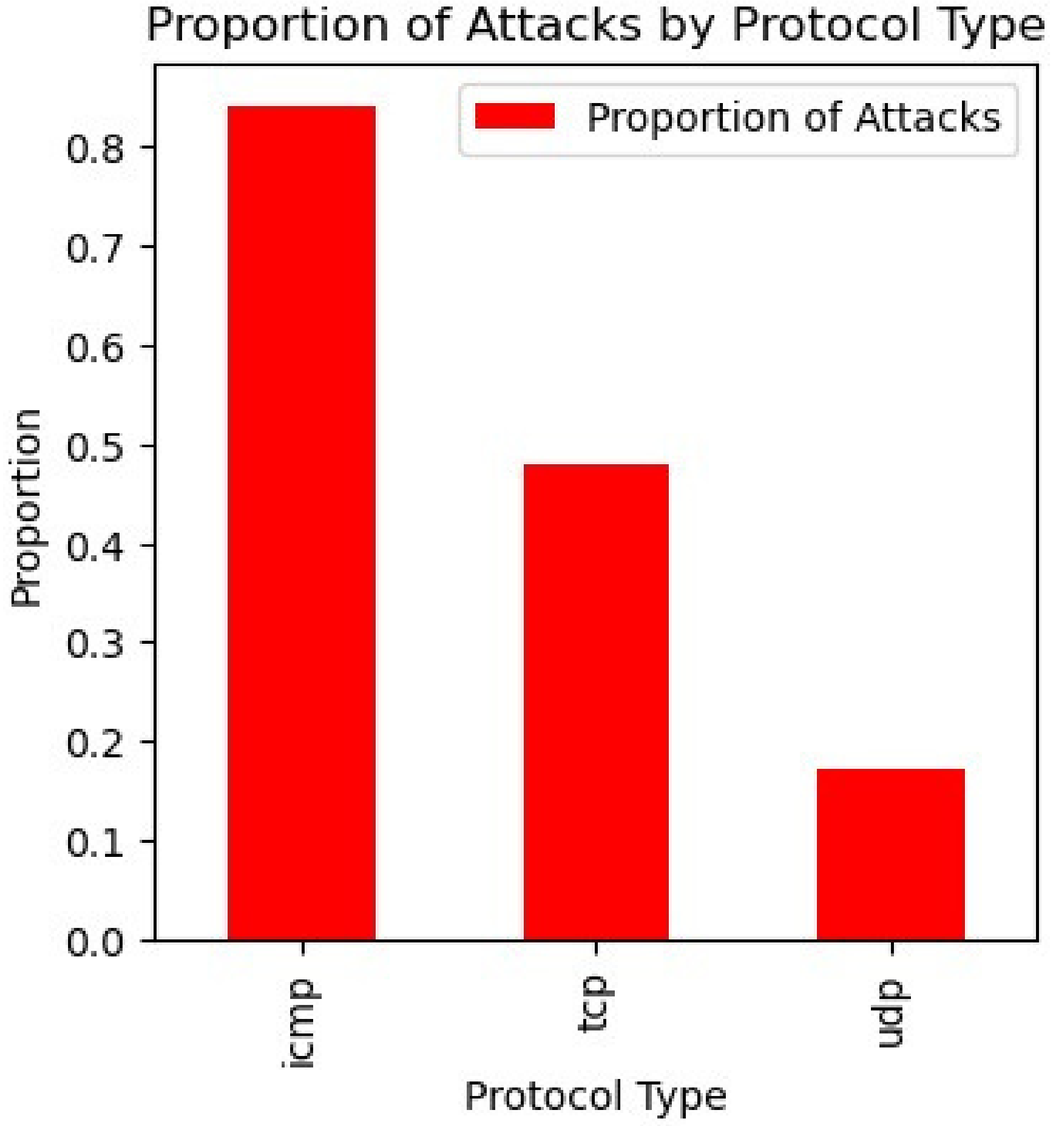
- We used the Random Forest classifier for model training
- Using this model, we detected the important features.
- The training was done on kdd-nsl data and validation was done through NS3 simulation on the trained model
- Below are some features that are marked as important by the model.

1. Number of unique services in a connection between Host-Client
2. Serror count (number of acknowledgment which shows unsuccessful connection)
3. Amount of data transferred (bytes)
4. Number of root logins in a Host-Client Link
5. Number of times the “su” command is attempted - Switch User

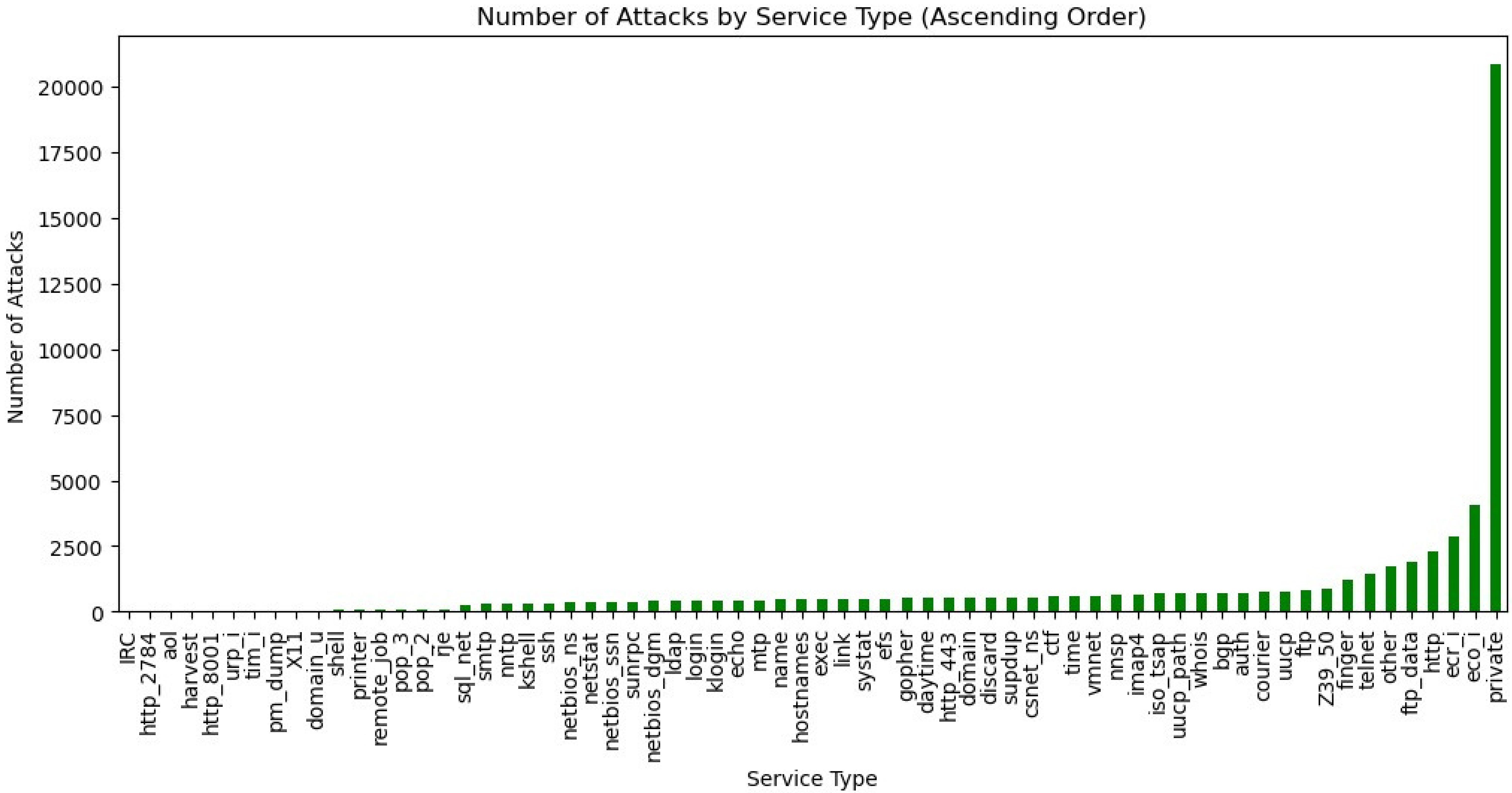
Identifying key features


Number of Packets by Protocol Type

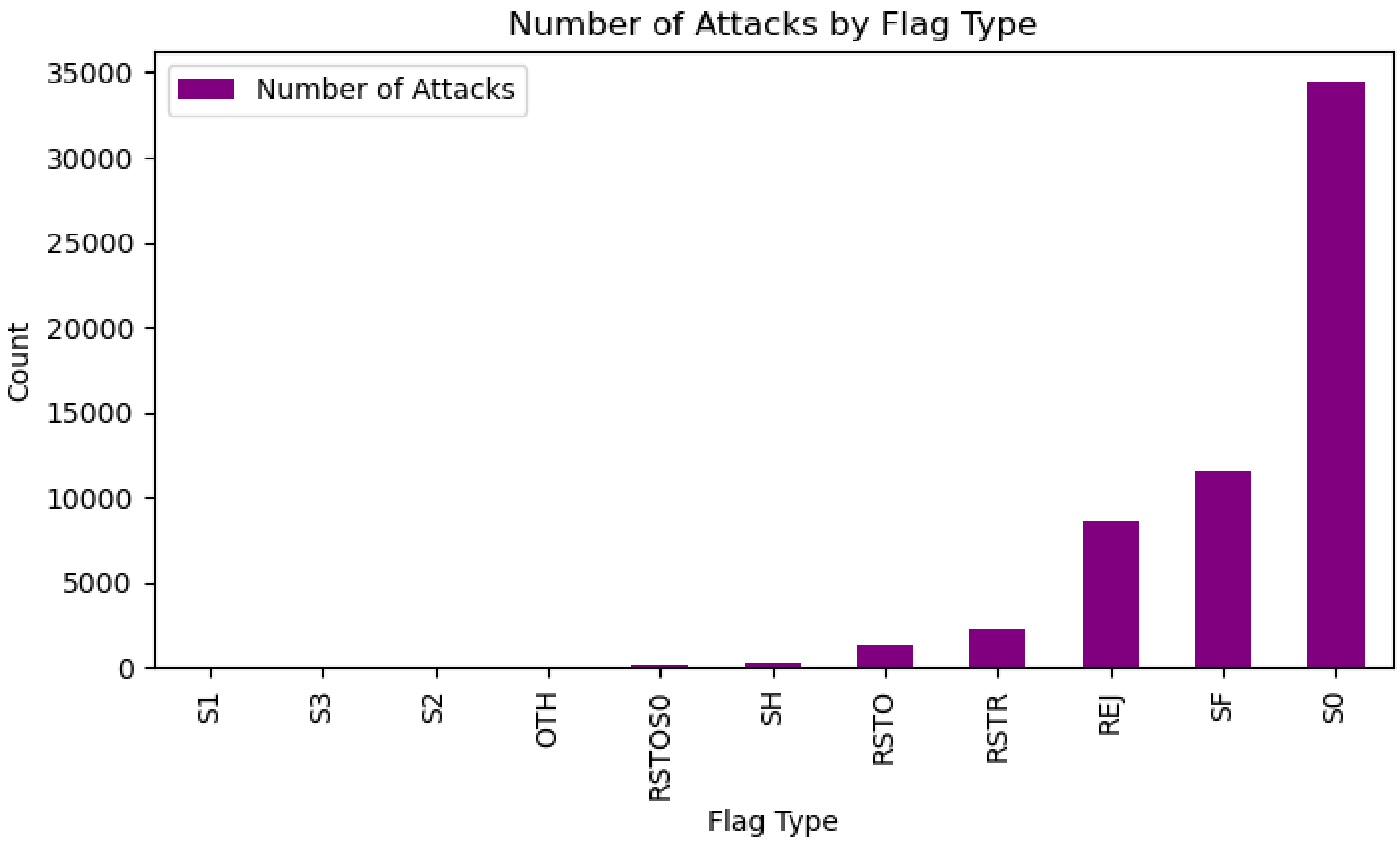

Number of Attacks by Protocol Type


Proportion of Attacks by Protocol Type

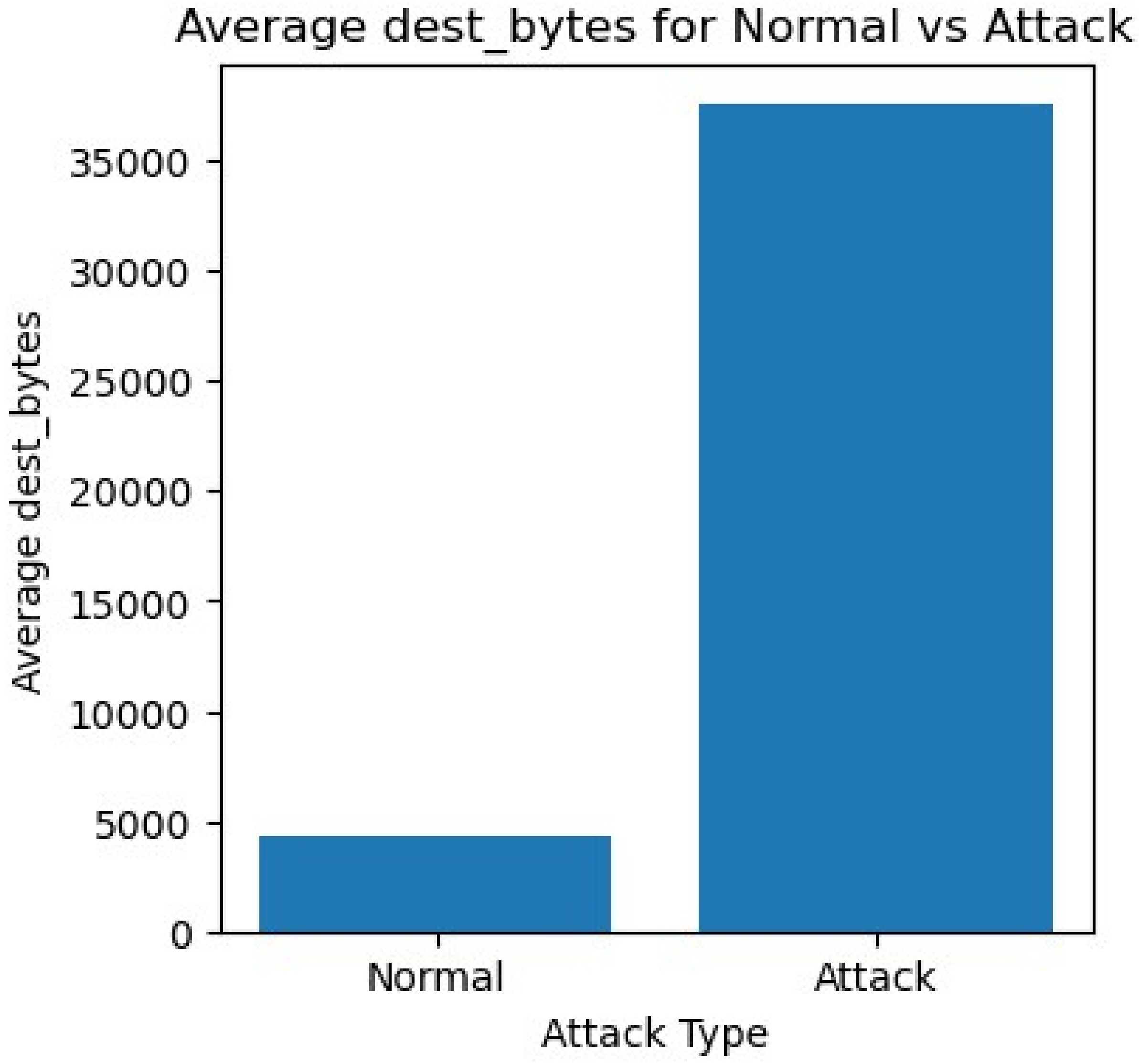
Identifying key features

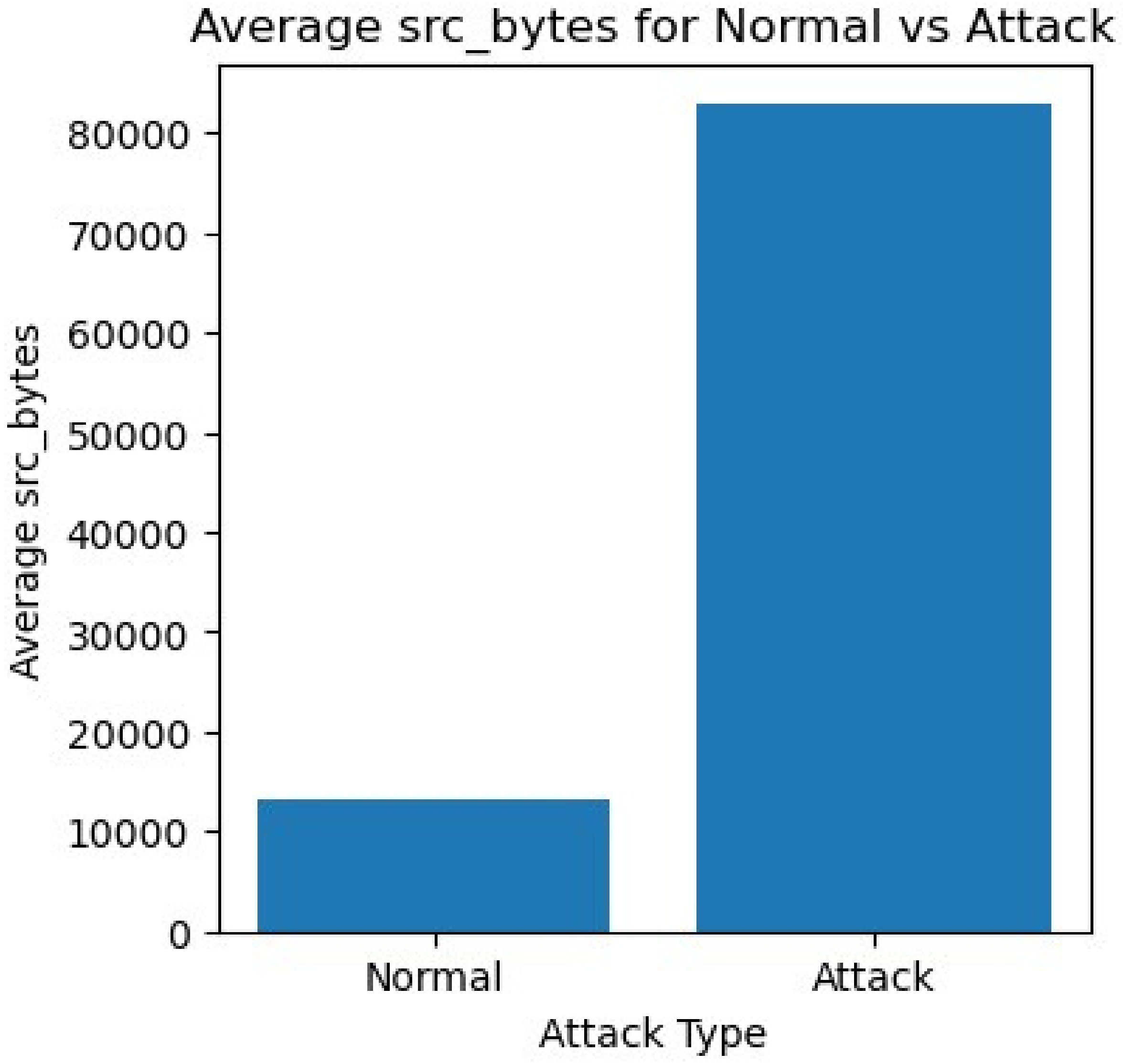


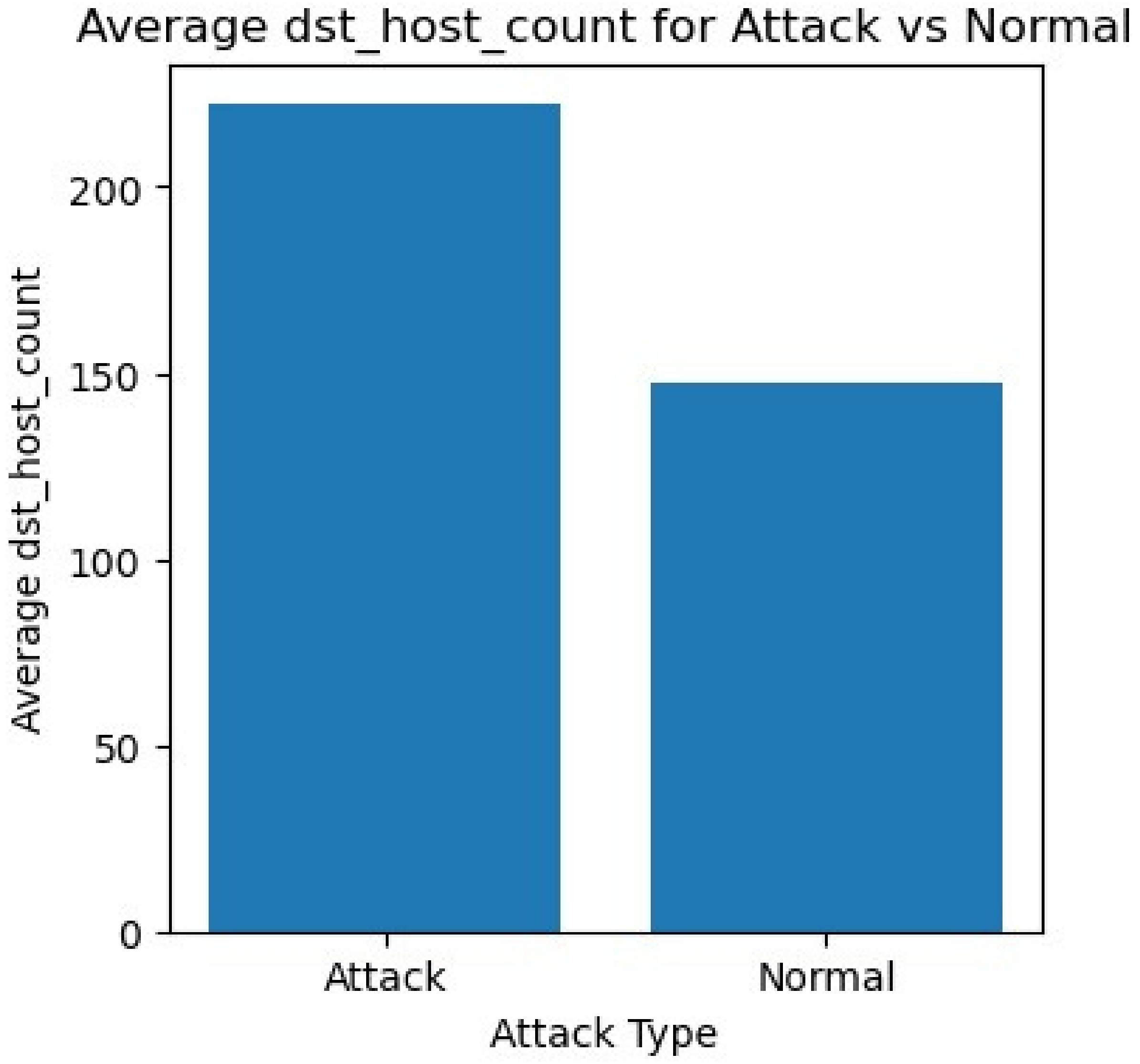
Identifying key features



Identifying key features


Average dest_bytes for Normal vs Attack


Average src_bytes for Normal vs Attack


Average dst_host_count for Attack vs Normal

References

- https://docs.google.com/document/d/13niCFlsB5B8U0cRcIGMET8f09nIftrCqstz9-M9Cho8/edit
- https://docs.google.com/spreadsheets/d/10_gCAfRcJN10x7-Z59qNFcSMceqjxD56U0ovqqarA/edit#gid=0
- https://paperswithcode.com/task/network-intrusion-detection
- https://github.com/nsnam/ns-3-dev-git
- https://www.nsnam.org/docs/models/ns-3-model-library.pdf
- https://ns3simulation.com/intrusion-detection-system-projects/
- https://github.com/Saket-Upadhyay/ns3-cybersecurity-simulations

Thank You