Data Card

• Name: UNSW-NB15 Dataset

• Type of Data: Network traffic data, containing features extracted from packet and flow data

• Contents: The dataset contains 2,540,044 rows of network traffic data, with 49 features per row. It includes both normal traffic and nine types of attacks.

• Source: The dataset was created by researchers at the University of New South Wales (UNSW) in Canberra, Australia.

• Creators: Nour Moustafa and Jill Slay

• Purpose: The dataset was created to support research in network intrusion detection and prevention systems.

• Collection Method: The data was generated by the IXIA PerfectStorm tool in the UNSW Cyber Range lab, simulating normal and attack traffic.

• Attacks Included: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms.

• Features: Features include flow features like duration, protocols, ports, and IP addresses as well as extracted features like number of bytes transferred.

• Availability: The dataset is publicly available for research purposes at https://research.unsw.edu.au/projects/unsw-nb15-dataset