Project: AI and Intrusion Detection

The topic of this project is AI (Artificial Intelligence) and intrusion detection with a focus on machine learning approaches. The use case is related to IoT (Internet of Things), where network traffic attacks were simulated on a real network. Using Wireshark, the data were filtered and structured in the form of a dataset (https://perso.esiee.fr/~omarm/datasets/Partial-IDS-IoT-Dataset.csv):

Feature	Description
Source_Port	Source port.
Destination_Port	Destination port.
Protocol	Protocol.
Flow_Duration	Flow duration.
Total_Forward_Packets	Number of the total packets in forward direction.
Total_Backward_Packets	Number of the total packets in backward direction.
Total_Length_Forward_Packets	Total size of packets in forward direction.
Total_Length_Backward_Packets	Total size of packets in backward direction.
Forward_Packets_Length_Max	Maximum size of packets in forward direction.
Forward_Packets_Length_Min	Minimum size of packets in forward direction.
Forward_Packets_Length_Mean	Mean size of packets in forward direction.
Backward_Packets_Length_Max	Maximum size of packets in backward direction.
Backward_Packets_Length_Min	Minimum size of packets in forward direction.
Backward_Packets_Length_Mean	Mean size of packets in backward direction.
Packets_Flow_IAT_Mean	Mean time between two flows.
Packets_Flow_IAT_Standard_Deviation	Standard deviation time between two flows of packets.
Packets_Flow_IAT_Max	Maximum time between two flows of packets.
Packets_Flow_IAT_Min	Minimum time between two flows of packets.
Forward_IAT_Total	Total time between two packets sent in forward direction.
Forward_IAT_Mean	Mean time between two packets sent in forward direction.
Forward_IAT_Min	Minimum time between two packets sent in forward direction.
Backward_IAT_Total	Total time between two packets sent in backward direction.
Backward_IAT_Mean	Mean time between two packets sent in backward direction.
Backward_IAT_Min	Minimum time between two packets sent in backward direction.
Forward_Header_Length	Total bytes used for headers in forward direction.
Backward_Header_Length	Total bytes used for headers in backward direction.

Forward_Packets_per_Second	Number of forward packets per second.
Backward_Packets_per_Second	Number of backward packets per second.
Packets_Length_Min	Minimum length of flow.
Packets_Length_Max	Maximum length of flow.
Packets_Length_Mean	Mean length of flow.
Packets_Length_Standard_Deviation	Standard deviation length of flow.
Class	Normal traffic or attack (Mirai, DoS, Scan, Spoofing)

Tasks:

1. Explain the attacks and discuss their impact in the context of IoT.
2. Using python, train a machine learning model upon these data and evaluate its performances. Explain each step.
3. Explain the relevance of each feature in intrusion detection.