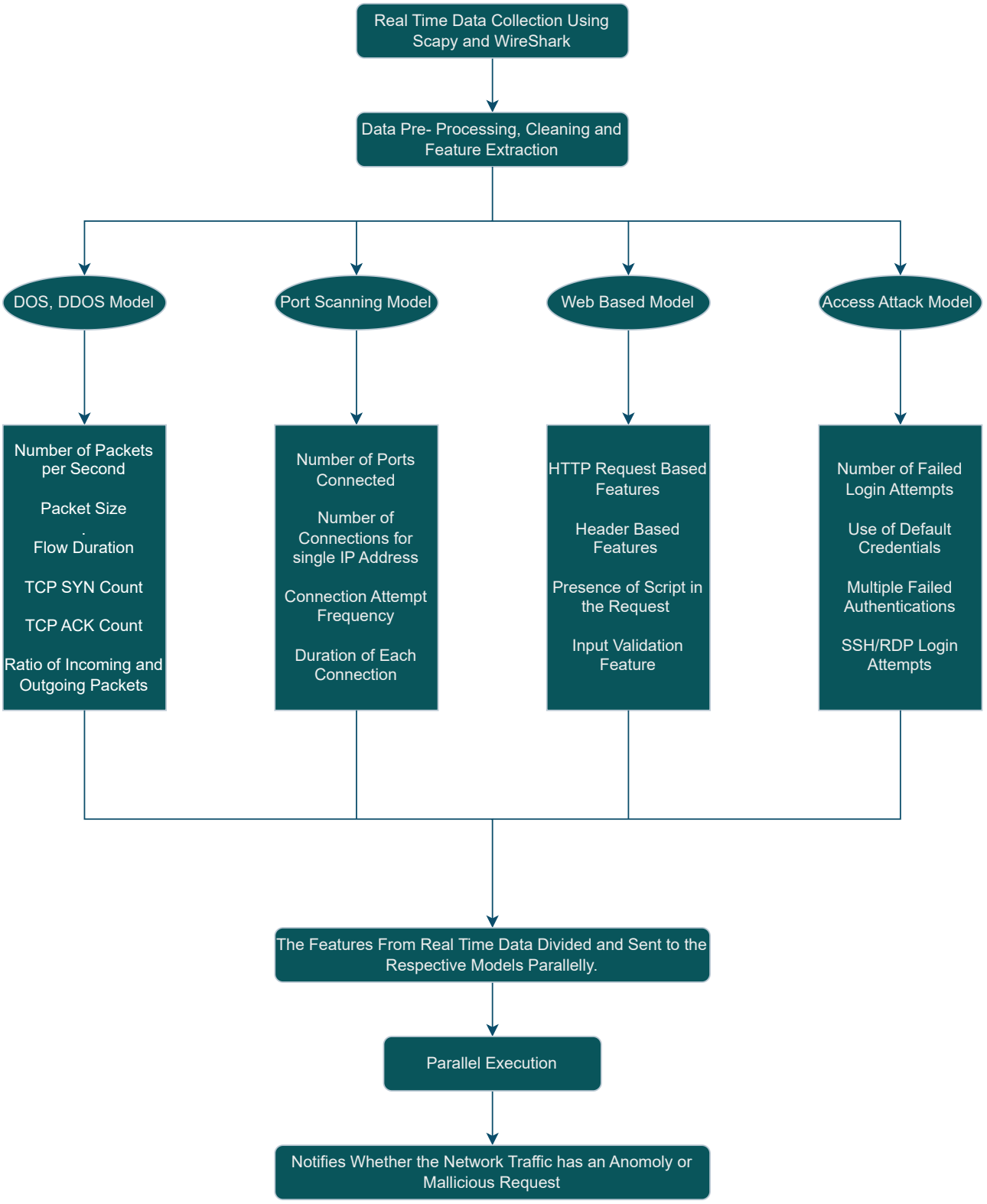
Real Time Data Collection Using Scapy and WireShark
Data Pre- Processing, Cleaning and Feature Extraction
DOS, DDOS Model
Port Scanning Model
Web Based Model
Access Attack Model
Number of Packets per Second
Packet Size
.
Flow Duration
TCP SYN Count
TCP ACK Count
Ratio of Incoming and Outgoing Packets
Number of Ports Connected
Number of Connections for single IP Address
Connection Attempt Frequency
Duration of Each Connection
HTTP Request Based Features
Header Based Features
Presence of Script in the Request
Input Validation Feature
Number of Failed Login Attempts
Use of Default Credentials
Multiple Failed Authentications
SSH/RDP Login Attempts
The Features From Real Time Data Divided and Sent to the Respective Models Parallelly.
Parallel Execution
Notifies Whether the Network Traffic has an Anomoly or Mallicious Request