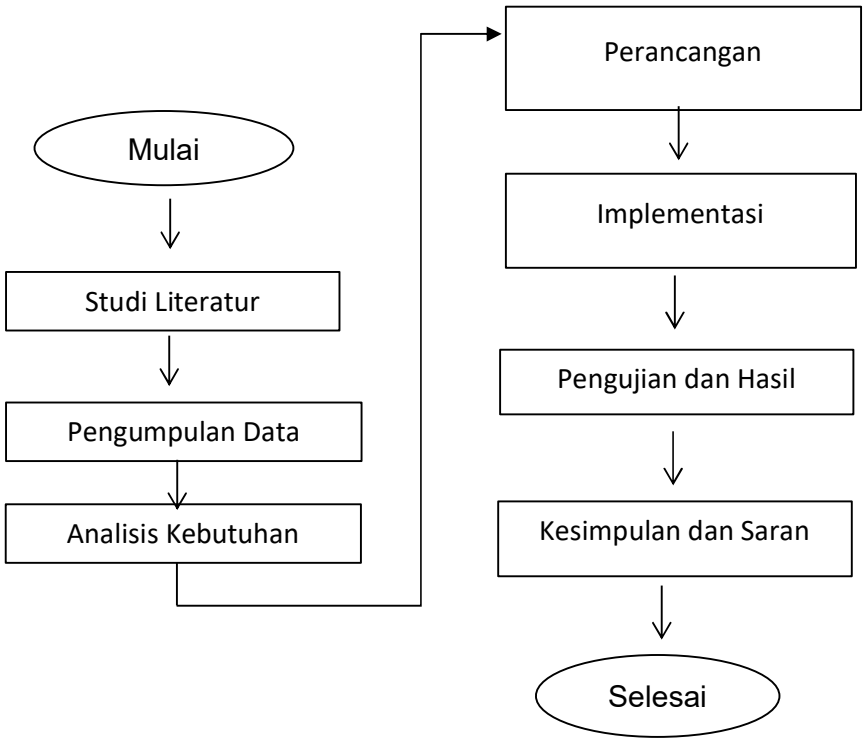
BAB 3 METODOLOGI

3.1 Alur Penelitian



Gambar 3.1 Alur penelitian

Gambar 3.1 merupakan langkah-langkah penelitian yang dikembangkan. Penelitian ini dimulai dari studi literatur, pengumpulan data, analisis kebutuhan, perancangan, implementasi, pengujian dan hasil, lalu diakhiri dengan penarikan kesimpulan dan saran.

3.2 Studi Literatur

Studi literatur dilakukan dengan meninjau penelitian terdahulu serta mendalami dasar teori yang berkaitan dengan pengembangan deteksi serangan DDoS berbasis *machine learning*. Informasi tersebut disadur melalui buku, jurnal ilmiah, dan situs internet terpercaya. Studi literatur yang dibutuhkan *Distributed Denial of Service*, *Intrusion Detection System*, *Machine Learning*, Algoritme C5.0, *Imbalancing Class*, Seleksi Fitur, dan Evaluasi Kinerja *Classifier*.

3.3 Pengumpulan Data

Data yang digunkan dalam penelitian ini adalah CICDDoS2019 yang dikembangkan oleh Fakultas Imu Komputer, Universitas New Brunswick pada tahun 2019. CICDDoS2019 berisi serangan DDoS umum yang jinak dan paling

mutakhir, yang menyerupai data pada dunia nyata yang sebenarnya (PCAP). Data ini juga terdiri dari hasil analisis lalu lintas jaringan menggunakan CICFlowMeter-V3 dengan aliran berlabel berdasarkan waktu, sumber, dan IP tujuan, port sumber dan tujuan, protokol dan serangan (file CSV). Tabel 3.1 berikut adalah fitur-fitur yang terdapat pada Dataset CICDDoS2019.

Tabel 3.1 Fitur pada Dataset CICDDoS2019

No.	Nama	No.	Nama
1.	Unnamed	44.	Bwd Packets/s
2.	Flow ID	45.	Min Packet Length
3.	Source IP	46.	Max Packet Length
4.	Source Port	47.	Packet Length Mean
5.	Destination IP	48.	Packet Length Std
6.	Destination Port	49.	Packet Length Variance
7.	Protocol	50.	FIN Flag Count
8.	Timestamp	51.	SYN Flag Count
9.	Flow Duration	52.	RST Flag Count
10.	Total Fwd Packet	53.	PSH Flag Count
11.	Total Backward Packet	54.	ACK Flag Count
12.	Total Length of Fwd Packets	55.	URG Flag Count
13.	Total Length of Bwd Packets	56.	CWE Flag Count
14.	Fwd Packet Length Max	57.	ECE Flag Count
15.	Fwd Packet Length Min	58.	Down/Up Ratio
16.	Fwd Packet Length Mean	59.	Average Packet Size
17.	Fwd Packet Length Std	60.	Avg Fwd Segment Size

Tabel 3.1 Fitur pada Dataset CICDDoS2019 (lanjutan)

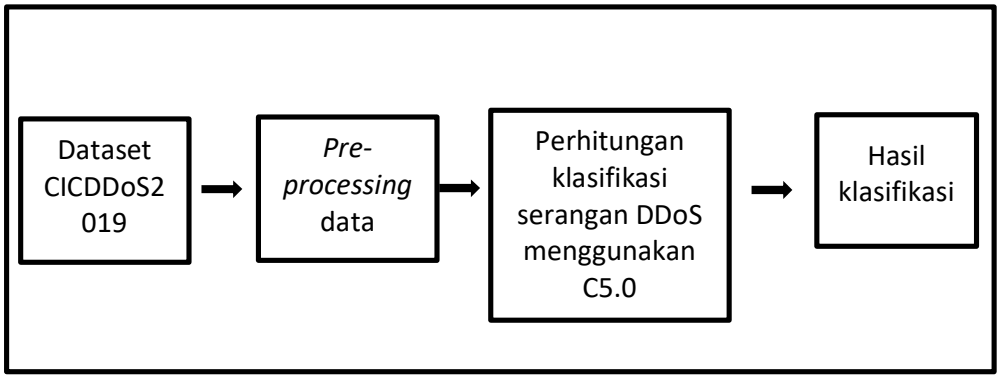
18.	Bwd Packet Length Max	61.	Avg Bwd Segment Size
19.	Bwd Packet Length Min	62.	Fwd Header Length.1
20.	Bwd Packet Length Mean	63.	Fwd Avg Bytes/Bulk
21.	Bwd Packet Length Std	64.	Fwd Avg Packets/Bulk
22.	Flow Bytes/s	65.	Fwd Avg Bulk Rate
23.	Flow Packets/s	66.	Bwd Avg Bytes/Bulk
24.	Flow IAT Mean	67.	Bwd Avg Packets/Bulk
25.	Flow IAT Std	68.	Bwd Avg Bulk Rate
26.	Flow IAT Max	69.	Subflow Fwd Packets
27.	Flow IAT Min	70.	Subflow Fwd Bytes
28.	Fwd IAT Total	71.	Subflow Bwd Packets
29.	Fwd IAT Mean	72.	Subflow Bwd Bytes
30.	Fwd IAT Std	73.	Init_Win_bytes_forward
31.	Fwd IAT Max	74.	Init_Win_bytes_backward
32.	Bwd IAT Total	75.	act_data_pkt_fwd
33.	Bwd IAT Mean	76.	min_seg_size_forward
34.	Bwd IAT Std	77.	Active Mean
35.	Bwd IAT Max	78.	Active Std
36.	Bwd IAT Min	79.	Active Max
37.	Fwd PSH Flags	80.	Active Min
38.	Bwd PSH Flags	81.	Idle Mean
39.	Fwd URG Flags	82.	Idle Std
40.	Bwd URG Flags	83.	Idle Max
41.	Fwd Header Length	84.	Idle Min
42.	Bwd Header Length	85.	SimillarHTTP
43.	Fwd Packets/s	86.	Inbound

3.4 Analisis Kebutuhan

Kebutuhan dari sistem ini adalah perangkat keras (*hardware*) dan perangkat lunak (*software*) yang diperlukan agar sistem berjalan dengan baik. Berikut ini spesifikasi dari perangakat keras dan perangkat lunak yakni:

1. Kebutuhan Perangkat Keras
   - Laptop atau Personal Computer (PC)
2. Kebutuhan Perangkat Lunak
   - Sistem Operasi Windows 10 64 bit sebagai lingkup kerja sistem.
   - Weka untuk *preprocessing* data.
   - Rstudio untuk mengimplementasikan algoritme klasifikasi
   - Ms. Excel 2019 untuk penyimpanan data.

3.5 Perancangan



Gambar 3.2 Perancangan Klasifikasi

Perancangan klasifikasi dapat digambarkan menggunakan diagram blok. Diagram blok menjelaskan aliran proses secara terstruktur, mulai dari input hingga output yang dihasilkan. Gambar 3.2 merupakan diagram blok yang dimulai dengan melakukan input dataset CICDDoS2019, kemudian dilanjutkan dengan pre-processing data yaitu seleksi fitur dan *balancing* dataset. Setelah itu melakukan klasifikasi menggunakan metode C5.0. Setelah proses dijalankan akan menghasilkan output klasifikasi.

3.6 Implementasi

Pada tahapan ini penelitian akan dibangun berdasarkan studi literatur yang sudah dikaji dan perancangan. Proses seleksi fitur dan *balancing* data menggunakan aplikasi Weka. Selanjutnya untuk melakukan klasifikasi serangan DDoS pada dataset CICDDoS 2019 menggunakan library C5.0 yang terdapat pada aplikasi R. Output yang diharapkan berupa hasil prediksi untuk diuji nilai akurasi, presisi, dan *recall*.

3.7 Pengujian dan Analisis

Pengujian yang akan dilakukan adalah pengujian validitas hasil, dan waktu yang dibutuhkan algoritme C5.0 dalam melakukan deteksi serangan.

3.7.1 Pengujian Perbandingan Rasio Data Latih dan Data Uji

Pengujian ini bertujuan untuk mengukur pengaruh akurasi terhadap pembagian rasio data latih dan data uji.

3.7.2 Pengujian Jumlah *Trial (Boosting)*

Pengujian jumlah *trial (boosting)* bertujuan untuk mengukur pengaruh akurasi terhadap jumlah *trial*. Pada kajian pustaka dijelaskan bahwa *boosting* mempengaruhi jumlah akurasi.

3.7.3 Pengujian Perbandingan *Confusion Matrix*

Untuk melakukan hasil pengujian validitas hasil menggunakan *single decision threshold* (*one feature*), fiturnya berupa kelas DDoS (serangan dan bukan serangan) seperti yang dijelaskan pada Tabel 3.2. Setelah nilai akurasi didapatkan, hasilnya akan dibandingkan dengan algoritme C5.0.

Tabel 3.2 Validitas menggunakan *single decision threshold*

Real / Prediksi	+	-
+	TP	FN
-	FP	TN

3.7.4 Pengujian Waktu Eksekusi

Pengujian waktu dilakukan untuk melihat durasi eksekusi yang dilakukan oleh algoritme dalam melakukan klasifikasi serangan.

3.8 Pengambilan Kesimpulan dan Saran

Dari hasil pengujian dan analisis maka ditarik kesimpulan bagaimana keberhasilan sistem ini ketika diimplementasikan dan terdapat beberapa saran untuk perbaikan sistem ini kedepannya.