EVALUASI SISTEM PENDETEKSI INTRUSI BERBASIS ANOMALI DENGAN N-GRAM DAN INCREMENTAL LEARNING

I Made Agus Adi Wirawan

5112 100 036

Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D.

Baskoro Adi Pratomo, S.Kom., M.Kom.

TEKNIK INFORMATIKA
INSTITUT TEKNOLOGI SEPULUH NOPEMBER

PENDAHULUAN

Rumusan Masalah

1. Bagaimana membangun sistem deteksi intrusi yang dapat membaca data set dari DARPA IDS tahun 1999 data set?
2. Bagaimana membangun sistem deteksi intrusi yang dapat menangkap paket data dari *network interface* suatu komputer?
3. Bagaimana menerapkan metode n-gram pada konten paket data?
4. Bagaimana cara mengklasifikasikan paket data menjadi dua kelompok, yaitu paket data normal dan paket data yang berupa intrusi dengan menggunakan metode Mahalanobis distance?
5. Bagaimana membangun sistem deteksi intrusi yang menerapkan metode *incremental learning*?

Batasan Masalah

1. Data set yang digunakan adalah DARPA IDS tahun 1999.
2. Jenis protokol yang diperiksa adalah TCP dengan port aplikasi dari FTP(21), Telnet(23), SMTP(25), HTTP(80) dan UDP dengan port aplikasi dari DNS Server(53).

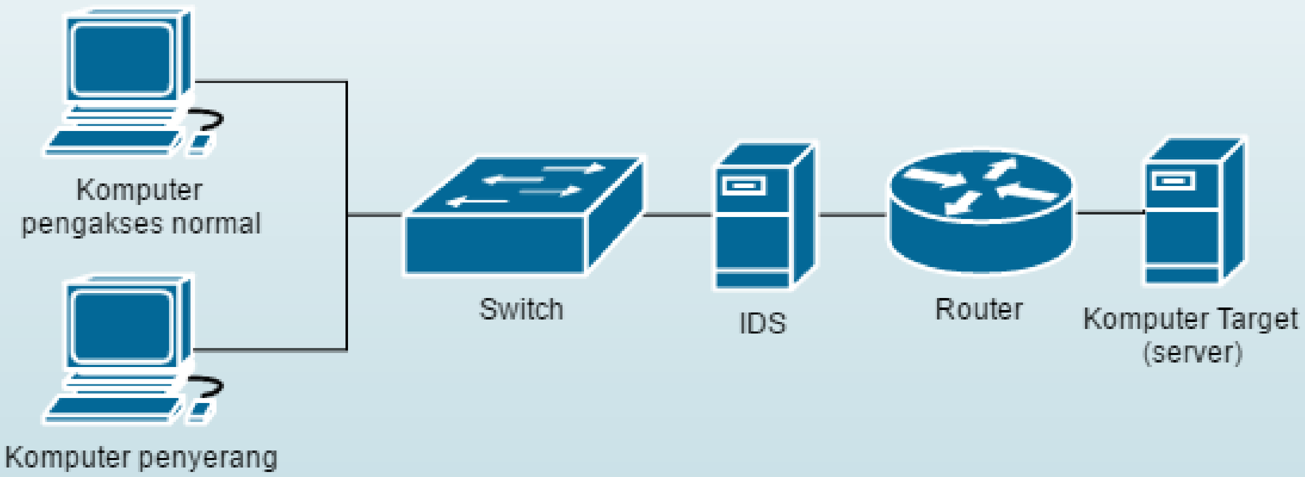
Tujuan

Membuat sistem pendeteksi intrusi yang mampu mengenali serangan pada lalu lintas jaringan dengan menggunakan metode Mahalanobis Distance berbasis anomali yang nantinya mampu membedakan paket data normal maupun paket data yang berupa intrusi.

DESAIN DAN IMPLEMENTASI

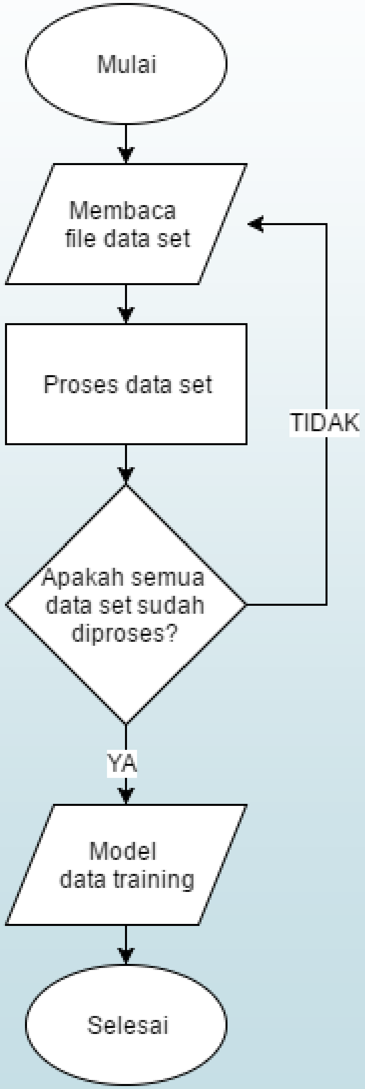
Desain Arsitektur Jaringan

- 1 router
- 1 komputer target
- 1 komputer pengakses normal
- 1 komputer penyerang



Proses Training Data Set

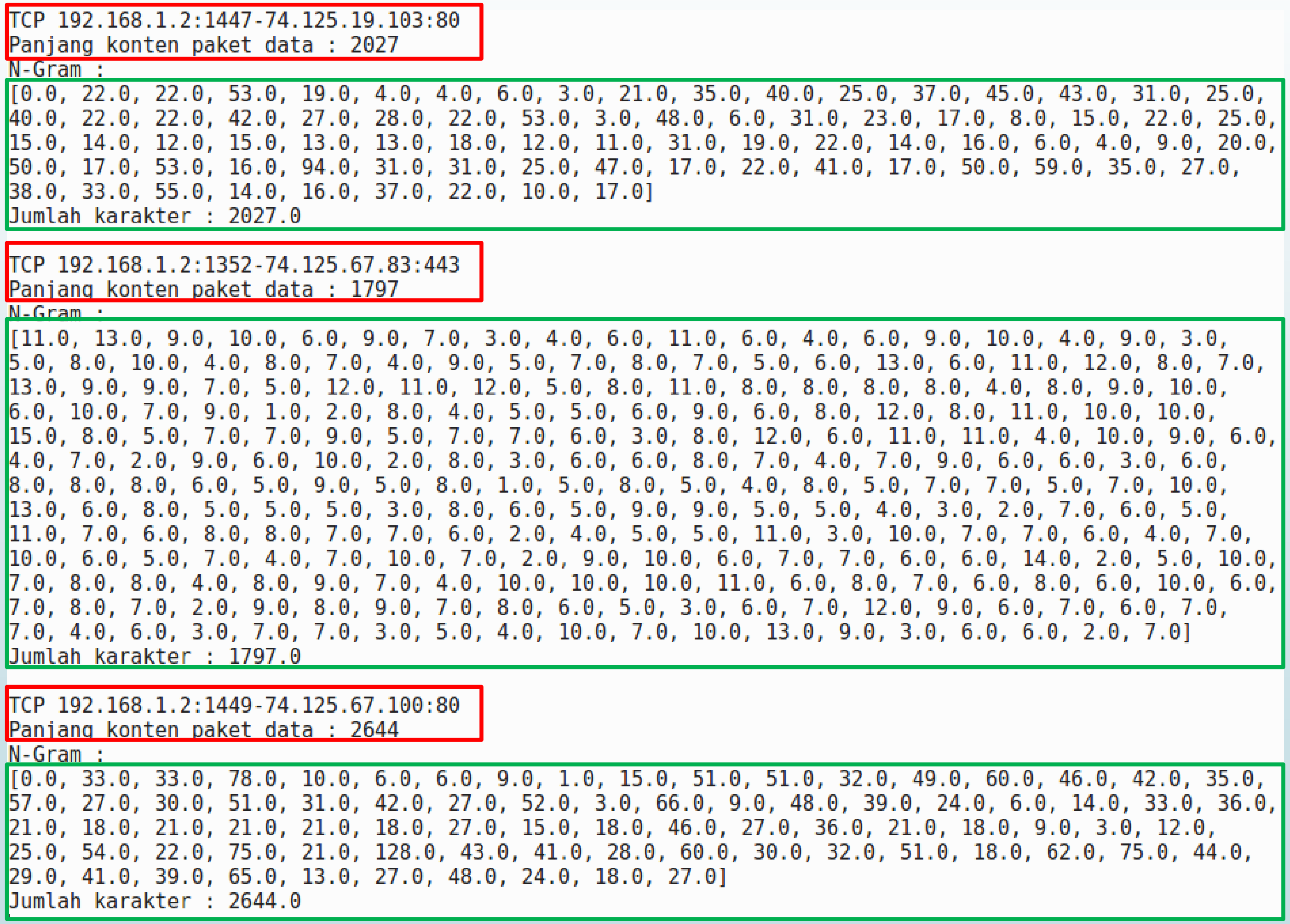
- Membaca file data set
- Rekonstruksi paket data
- Membuat model data training



Implementasi Proses N-Gram

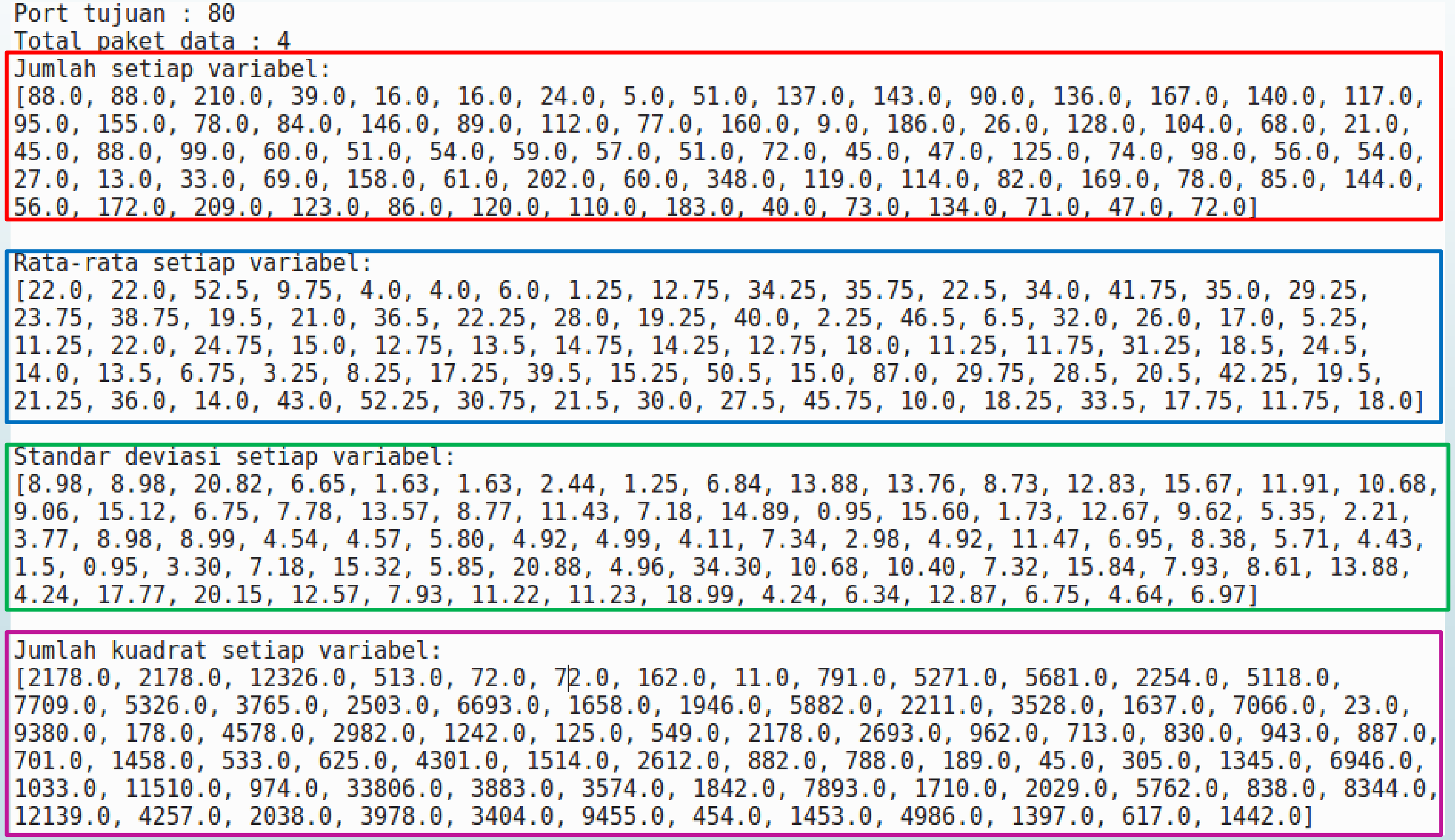
```
1 Terima konten paket menggunakan fungsi Ngram()
2 Deklarasi double[] n = new doublbe[256];
3 Baca konten paket
4 Konversi konten paket data menjadi unsign integer
5 Tambahkan 1 ke n setiap konten paket yang sesuai
```

Implementasi Proses N-Gram (2)



```
TCP 192.168.1.2:1447-74.125.19.103:80
Panjang konten paket data : 2027
N-Gram :
[0.0, 22.0, 22.0, 53.0, 19.0, 4.0, 4.0, 6.0, 3.0, 21.0, 35.0, 40.0, 25.0, 37.0, 45.0, 43.0, 31.0, 25.0,
40.0, 22.0, 22.0, 42.0, 27.0, 28.0, 22.0, 53.0, 3.0, 48.0, 6.0, 31.0, 23.0, 17.0, 8.0, 15.0, 22.0, 25.0,
15.0, 14.0, 12.0, 15.0, 13.0, 13.0, 18.0, 12.0, 11.0, 31.0, 19.0, 22.0, 14.0, 16.0, 6.0, 4.0, 9.0, 20.0,
50.0, 17.0, 53.0, 16.0, 94.0, 31.0, 31.0, 25.0, 47.0, 17.0, 22.0, 41.0, 17.0, 50.0, 59.0, 35.0, 27.0,
38.0, 33.0, 55.0, 14.0, 16.0, 37.0, 22.0, 10.0, 17.0]
Jumlah karakter : 2027.0

TCP 192.168.1.2:1352-74.125.67.83:443
Panjang konten paket data : 1797
N-Gram :
[11.0, 13.0, 9.0, 10.0, 6.0, 9.0, 7.0, 3.0, 4.0, 6.0, 11.0, 6.0, 4.0, 6.0, 9.0, 10.0, 4.0, 9.0, 3.0,
5.0, 8.0, 10.0, 4.0, 8.0, 7.0, 4.0, 9.0, 5.0, 7.0, 8.0, 7.0, 5.0, 6.0, 13.0, 6.0, 11.0, 12.0, 8.0, 7.0,
13.0, 9.0, 9.0, 7.0, 5.0, 12.0, 11.0, 12.0, 5.0, 8.0, 11.0, 8.0, 8.0, 8.0, 8.0, 4.0, 8.0, 9.0, 10.0,
6.0, 10.0, 7.0, 9.0, 1.0, 2.0, 8.0, 4.0, 5.0, 5.0, 6.0, 9.0, 6.0, 8.0, 12.0, 8.0, 11.0, 10.0, 10.0,
15.0, 8.0, 5.0, 7.0, 7.0, 9.0, 5.0, 7.0, 7.0, 6.0, 3.0, 8.0, 12.0, 6.0, 11.0, 11.0, 4.0, 10.0, 9.0, 6.0,
4.0, 7.0, 2.0, 9.0, 6.0, 10.0, 2.0, 8.0, 3.0, 6.0, 6.0, 8.0, 7.0, 4.0, 7.0, 9.0, 6.0, 6.0, 3.0, 6.0,
8.0, 8.0, 8.0, 6.0, 5.0, 9.0, 5.0, 8.0, 1.0, 5.0, 8.0, 5.0, 4.0, 8.0, 5.0, 7.0, 7.0, 5.0, 7.0, 10.0,
13.0, 6.0, 8.0, 5.0, 5.0, 5.0, 3.0, 8.0, 6.0, 5.0, 9.0, 9.0, 5.0, 5.0, 4.0, 3.0, 2.0, 7.0, 6.0, 5.0,
11.0, 7.0, 6.0, 8.0, 8.0, 7.0, 7.0, 6.0, 2.0, 4.0, 5.0, 5.0, 11.0, 3.0, 10.0, 7.0, 7.0, 6.0, 4.0, 7.0,
10.0, 6.0, 5.0, 7.0, 4.0, 7.0, 10.0, 7.0, 2.0, 9.0, 10.0, 6.0, 7.0, 7.0, 6.0, 6.0, 14.0, 2.0, 5.0, 10.0,
7.0, 8.0, 8.0, 4.0, 8.0, 9.0, 7.0, 4.0, 10.0, 10.0, 10.0, 11.0, 6.0, 8.0, 7.0, 6.0, 8.0, 6.0, 10.0, 6.0,
7.0, 8.0, 7.0, 2.0, 9.0, 8.0, 9.0, 7.0, 8.0, 6.0, 5.0, 3.0, 6.0, 7.0, 12.0, 9.0, 6.0, 7.0, 6.0, 7.0,
7.0, 4.0, 6.0, 3.0, 7.0, 7.0, 3.0, 5.0, 4.0, 10.0, 7.0, 10.0, 13.0, 9.0, 3.0, 6.0, 6.0, 2.0, 7.0]
Jumlah karakter : 1797.0

TCP 192.168.1.2:1449-74.125.67.100:80
Panjang konten paket data : 2644
N-Gram :
[0.0, 33.0, 33.0, 78.0, 10.0, 6.0, 6.0, 9.0, 1.0, 15.0, 51.0, 51.0, 32.0, 49.0, 60.0, 46.0, 42.0, 35.0,
57.0, 27.0, 30.0, 51.0, 31.0, 42.0, 27.0, 52.0, 3.0, 66.0, 9.0, 48.0, 39.0, 24.0, 6.0, 14.0, 33.0, 36.0,
21.0, 18.0, 21.0, 21.0, 21.0, 18.0, 27.0, 15.0, 18.0, 46.0, 27.0, 36.0, 21.0, 18.0, 9.0, 3.0, 12.0,
25.0, 54.0, 22.0, 75.0, 21.0, 128.0, 43.0, 41.0, 28.0, 60.0, 30.0, 32.0, 51.0, 18.0, 62.0, 75.0, 44.0,
29.0, 41.0, 39.0, 65.0, 13.0, 27.0, 48.0, 24.0, 18.0, 27.0]
Jumlah karakter : 2644.0
```

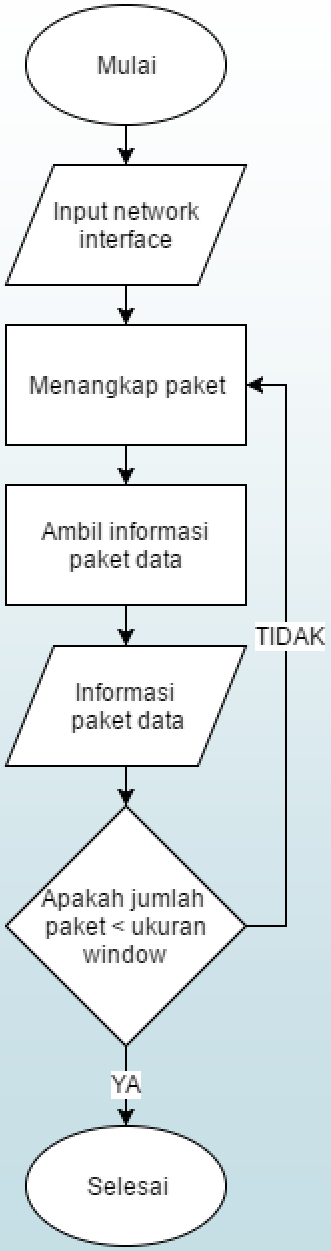
Implementasi Pembuatan Model Data Training



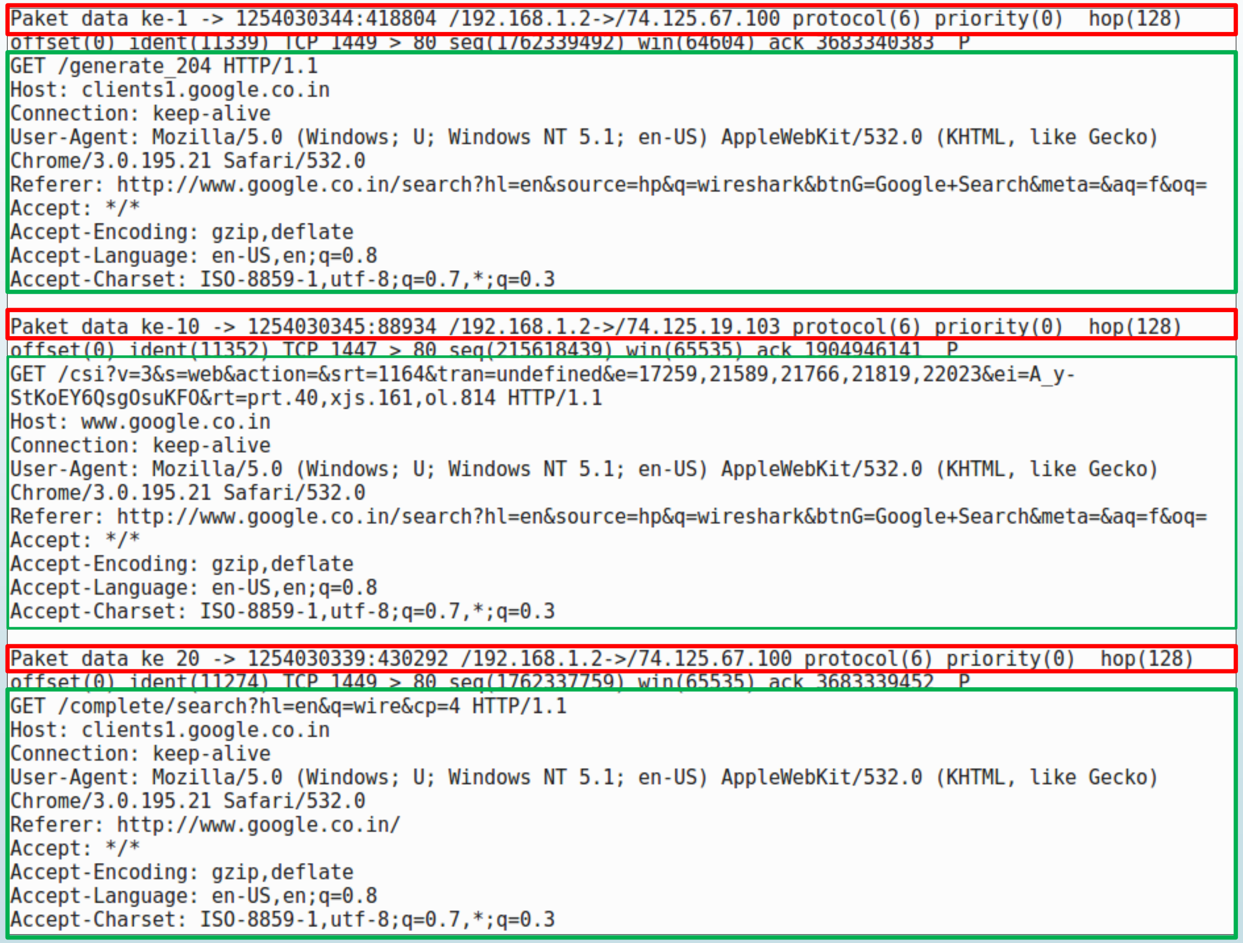
```
Port tujuan : 80
Total paket data : 4
Jumlah setiap variabel:
[88.0, 88.0, 210.0, 39.0, 16.0, 16.0, 24.0, 5.0, 51.0, 137.0, 143.0, 90.0, 136.0, 167.0, 140.0, 117.0,
95.0, 155.0, 78.0, 84.0, 146.0, 89.0, 112.0, 77.0, 160.0, 9.0, 186.0, 26.0, 128.0, 104.0, 68.0, 21.0,
45.0, 88.0, 99.0, 60.0, 51.0, 54.0, 59.0, 57.0, 51.0, 72.0, 45.0, 47.0, 125.0, 74.0, 98.0, 56.0, 54.0,
27.0, 13.0, 33.0, 69.0, 158.0, 61.0, 202.0, 60.0, 348.0, 119.0, 114.0, 82.0, 169.0, 78.0, 85.0, 144.0,
56.0, 172.0, 209.0, 123.0, 86.0, 120.0, 110.0, 183.0, 40.0, 73.0, 134.0, 71.0, 47.0, 72.0]

Rata-rata setiap variabel:
[22.0, 22.0, 52.5, 9.75, 4.0, 4.0, 6.0, 1.25, 12.75, 34.25, 35.75, 22.5, 34.0, 41.75, 35.0, 29.25,
23.75, 38.75, 19.5, 21.0, 36.5, 22.25, 28.0, 19.25, 40.0, 2.25, 46.5, 6.5, 32.0, 26.0, 17.0, 5.25,
11.25, 22.0, 24.75, 15.0, 12.75, 13.5, 14.75, 14.25, 12.75, 18.0, 11.25, 11.75, 31.25, 18.5, 24.5,
14.0, 13.5, 6.75, 3.25, 8.25, 17.25, 39.5, 15.25, 50.5, 15.0, 87.0, 29.75, 28.5, 20.5, 42.25, 19.5,
21.25, 36.0, 14.0, 43.0, 52.25, 30.75, 21.5, 30.0, 27.5, 45.75, 10.0, 18.25, 33.5, 17.75, 11.75, 18.0]

Standar deviasi setiap variabel:
[8.98, 8.98, 20.82, 6.65, 1.63, 1.63, 2.44, 1.25, 6.84, 13.88, 13.76, 8.73, 12.83, 15.67, 11.91, 10.68,
9.06, 15.12, 6.75, 7.78, 13.57, 8.77, 11.43, 7.18, 14.89, 0.95, 15.60, 1.73, 12.67, 9.62, 5.35, 2.21,
3.77, 8.98, 8.99, 4.54, 4.57, 5.80, 4.92, 4.99, 4.11, 7.34, 2.98, 4.92, 11.47, 6.95, 8.38, 5.71, 4.43,
1.5, 0.95, 3.30, 7.18, 15.32, 5.85, 20.88, 4.96, 34.30, 10.68, 10.40, 7.32, 15.84, 7.93, 8.61, 13.88,
4.24, 17.77, 20.15, 12.57, 7.93, 11.22, 11.23, 18.99, 4.24, 6.34, 12.87, 6.75, 4.64, 6.97]

Jumlah kuadrat setiap variabel:
[2178.0, 2178.0, 12326.0, 513.0, 72.0, 72.0, 162.0, 11.0, 791.0, 5271.0, 5681.0, 2254.0, 5118.0,
7709.0, 5326.0, 3765.0, 2503.0, 6693.0, 1658.0, 1946.0, 5882.0, 2211.0, 3528.0, 1637.0, 7066.0, 23.0,
9380.0, 178.0, 4578.0, 2982.0, 1242.0, 125.0, 549.0, 2178.0, 2693.0, 962.0, 713.0, 830.0, 943.0, 887.0,
701.0, 1458.0, 533.0, 625.0, 4301.0, 1514.0, 2612.0, 882.0, 788.0, 189.0, 45.0, 305.0, 1345.0, 6946.0,
1033.0, 11510.0, 974.0, 33806.0, 3883.0, 3574.0, 1842.0, 7893.0, 1710.0, 2029.0, 5762.0, 838.0, 8344.0,
12139.0, 4257.0, 2038.0, 3978.0, 3404.0, 9455.0, 454.0, 1453.0, 4986.0, 1397.0, 617.0, 1442.0]
```

Proses Penangkapan Paket

- Pilih metode input paket data
- Menangkap paket data
- Menyimpan informasi paket data



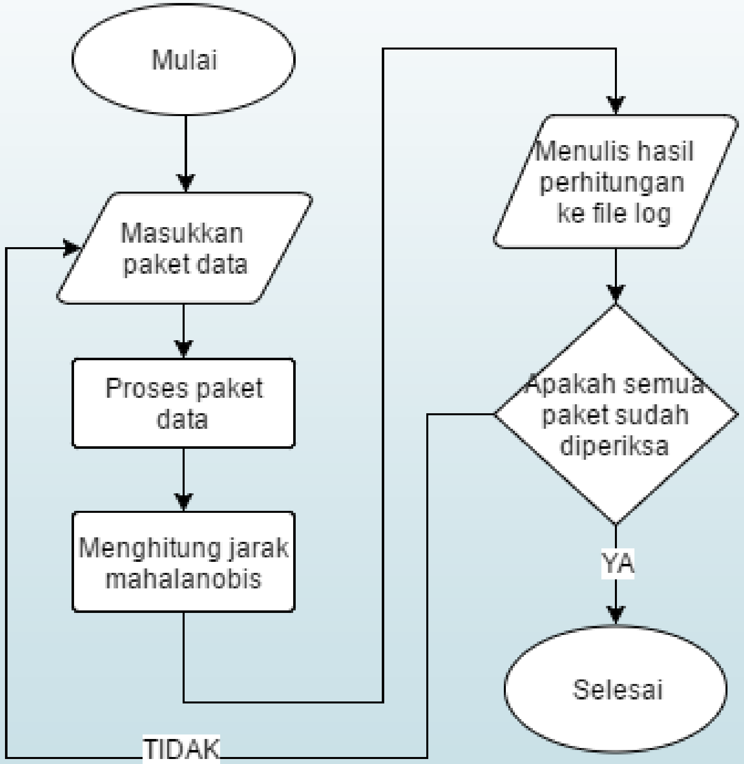
Implementasi Proses Sniffing



```
Paket data ke-1 -> 1254030344:418804 /192.168.1.2->/74.125.67.100 protocol(6) priority(0)  hop(128)
offset(0) ident(11339) TCP 1449 > 80 seq(1762339492) win(64604) ack 3683340383  P
GET /generate_204 HTTP/1.1
Host: clients1.google.co.in
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.0 (KHTML, like Gecko)
Chrome/3.0.195.21 Safari/532.0
Referer: http://www.google.co.in/search?hl=en&source=hp&q=wireshark&btnG=Google+Search&meta=&aq=f&oq=
Accept: */*
Accept-Encoding: gzip,deflate
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

Paket data ke-10 -> 1254030345:88934 /192.168.1.2->/74.125.19.103 protocol(6) priority(0)  hop(128)
offset(0) ident(11352) TCP 1447 > 80 seq(215618439) win(65535) ack 1904946141  P
GET /csi?v=3&s=web&action=&srt=1164&tran=undefined&e=17259,21589,21766,21819,22023&ei=A_y-
StKoEY6QsgOsuKFO&rt=prt.40,xjs.161,ol.814 HTTP/1.1
Host: www.google.co.in
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.0 (KHTML, like Gecko)
Chrome/3.0.195.21 Safari/532.0
Referer: http://www.google.co.in/search?hl=en&source=hp&q=wireshark&btnG=Google+Search&meta=&aq=f&oq=
Accept: */*
Accept-Encoding: gzip,deflate
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

Paket data ke 20 -> 1254030339:430292 /192.168.1.2->/74.125.67.100 protocol(6) priority(0)  hop(128)
offset(0) ident(11274) TCP 1449 > 80 seq(1762337759) win(65535) ack 3683339452  P
GET /complete/search?hl=en&q=wire&cp=4 HTTP/1.1
Host: clients1.google.co.in
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.0 (KHTML, like Gecko)
Chrome/3.0.195.21 Safari/532.0
Referer: http://www.google.co.in/
Accept: */*
Accept-Encoding: gzip,deflate
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
```

Proses Identifikasi

- Masukkan paket data
- Menghitung jarak mahalanobis
- Membandingkan jarak mahalanobis dengan nilai threshold
- Menulis hasil perhitungan ke file log


Mulai
Masukkan paket data
Proses paket data
Menghitung jarak mahalanobis
Menulis hasil perhitungan ke file log
Apakah semua paket sudah diperiksa
YA
Selesai
TIDAK

Mahalnobis Distance

$$d(x,\overline{y}) = \sum_{i=0}^{n-1}(|x_i - \overline{y_i}|/(\overline{\sigma_i} + \alpha))$$

d = jarak mahalanobis

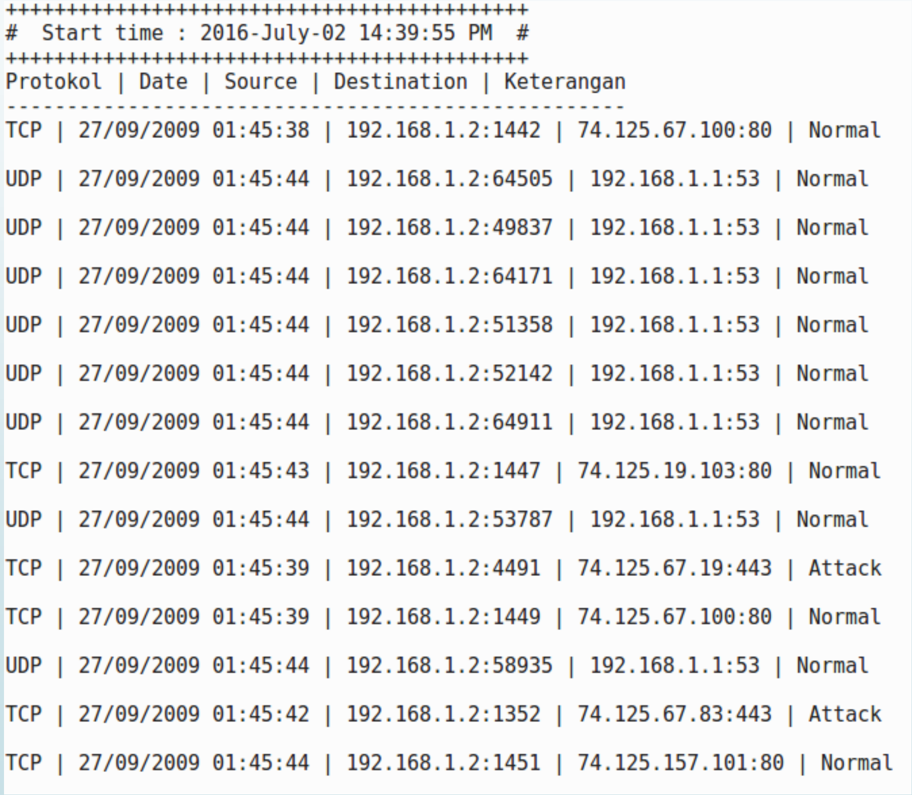
x_i = variable ke-i dari *payload* baru

$\overline{y_i}$ = rata-rata variable ke-i dari model data *training*

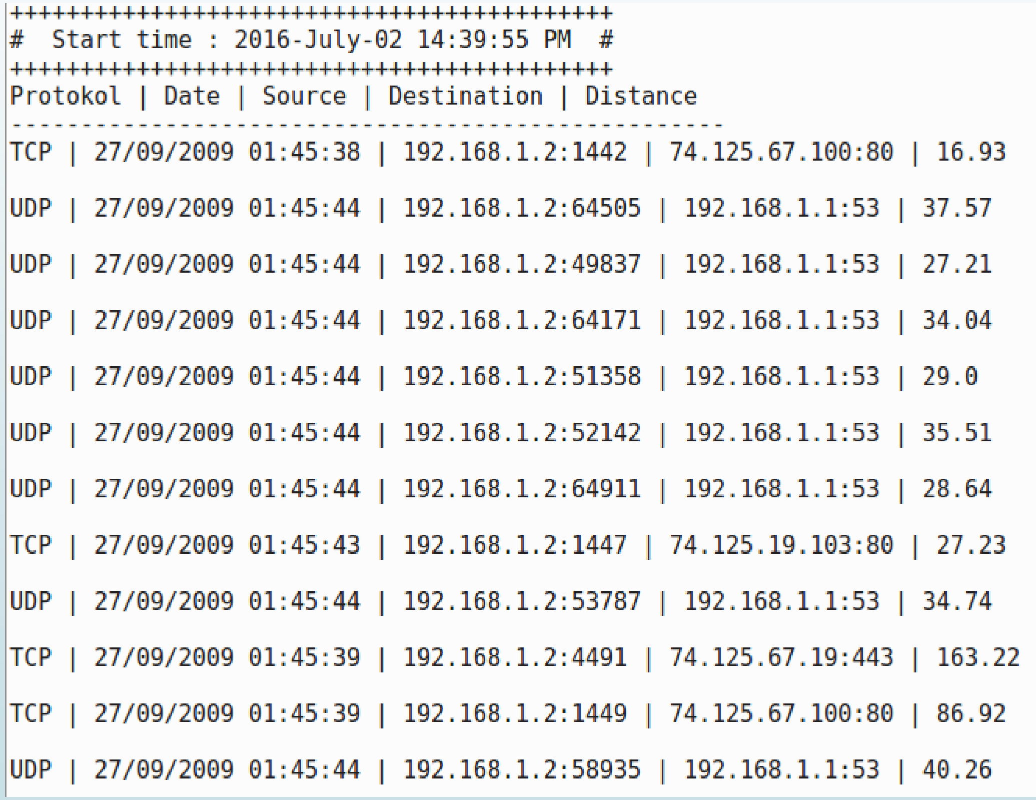
$\overline{\sigma_i}$ = standar deviasi variable ke-i dari model data *training*

α = *smoothing factor*

Implementasi Proses Identifikasi

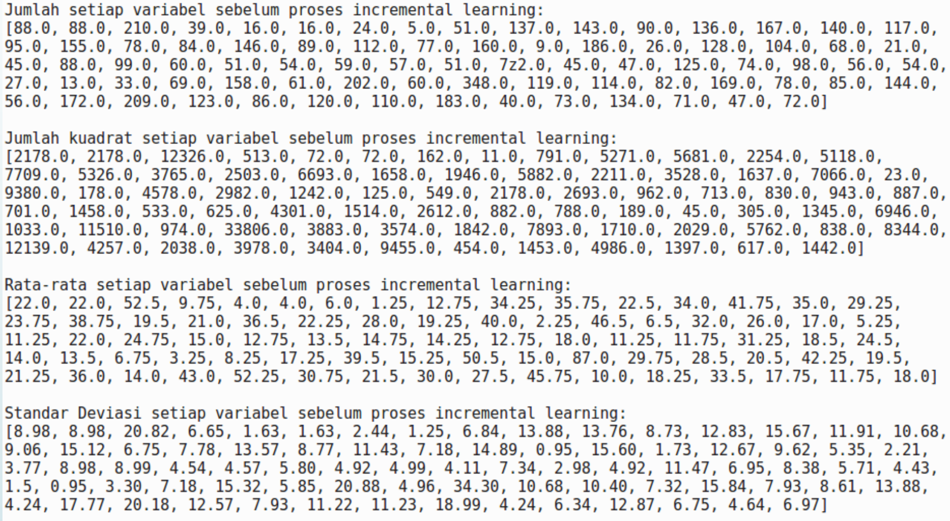


```
+++++++++++++++++++++++++++++++++++++++++++
#  Start time : 2016-July-02 14:39:55 PM  #
+++++++++++++++++++++++++++++++++++++++++++
Protokol | Date | Source | Destination | Keterangan
---------------------------------------------------
TCP | 27/09/2009 01:45:38 | 192.168.1.2:1442 | 74.125.67.100:80 | Normal

UDP | 27/09/2009 01:45:44 | 192.168.1.2:64505 | 192.168.1.1:53 | Normal

UDP | 27/09/2009 01:45:44 | 192.168.1.2:49837 | 192.168.1.1:53 | Normal

UDP | 27/09/2009 01:45:44 | 192.168.1.2:64171 | 192.168.1.1:53 | Normal

UDP | 27/09/2009 01:45:44 | 192.168.1.2:51358 | 192.168.1.1:53 | Normal

UDP | 27/09/2009 01:45:44 | 192.168.1.2:52142 | 192.168.1.1:53 | Normal

UDP | 27/09/2009 01:45:44 | 192.168.1.2:64911 | 192.168.1.1:53 | Normal

TCP | 27/09/2009 01:45:43 | 192.168.1.2:1447 | 74.125.19.103:80 | Normal

UDP | 27/09/2009 01:45:44 | 192.168.1.2:53787 | 192.168.1.1:53 | Normal

TCP | 27/09/2009 01:45:39 | 192.168.1.2:4491 | 74.125.67.19:443 | Attack

TCP | 27/09/2009 01:45:39 | 192.168.1.2:1449 | 74.125.67.100:80 | Normal

UDP | 27/09/2009 01:45:44 | 192.168.1.2:58935 | 192.168.1.1:53 | Normal

TCP | 27/09/2009 01:45:42 | 192.168.1.2:1352 | 74.125.67.83:443 | Attack

TCP | 27/09/2009 01:45:44 | 192.168.1.2:1451 | 74.125.157.101:80 | Normal
```



```
+++++++++++++++++++++++++++++++++++++++++++
#  Start time : 2016-July-02 14:39:55 PM  #
+++++++++++++++++++++++++++++++++++++++++++
Protokol | Date | Source | Destination | Distance
-------------------------------------------------
TCP | 27/09/2009 01:45:38 | 192.168.1.2:1442 | 74.125.67.100:80 | 16.93

UDP | 27/09/2009 01:45:44 | 192.168.1.2:64505 | 192.168.1.1:53 | 37.57

UDP | 27/09/2009 01:45:44 | 192.168.1.2:49837 | 192.168.1.1:53 | 27.21

UDP | 27/09/2009 01:45:44 | 192.168.1.2:64171 | 192.168.1.1:53 | 34.04

UDP | 27/09/2009 01:45:44 | 192.168.1.2:51358 | 192.168.1.1:53 | 29.0

UDP | 27/09/2009 01:45:44 | 192.168.1.2:52142 | 192.168.1.1:53 | 35.51

UDP | 27/09/2009 01:45:44 | 192.168.1.2:64911 | 192.168.1.1:53 | 28.64

TCP | 27/09/2009 01:45:43 | 192.168.1.2:1447 | 74.125.19.103:80 | 27.23

UDP | 27/09/2009 01:45:44 | 192.168.1.2:53787 | 192.168.1.1:53 | 34.74

TCP | 27/09/2009 01:45:39 | 192.168.1.2:4491 | 74.125.67.19:443 | 163.22

TCP | 27/09/2009 01:45:39 | 192.168.1.2:1449 | 74.125.67.100:80 | 86.92

UDP | 27/09/2009 01:45:44 | 192.168.1.2:58935 | 192.168.1.1:53 | 40.26
```

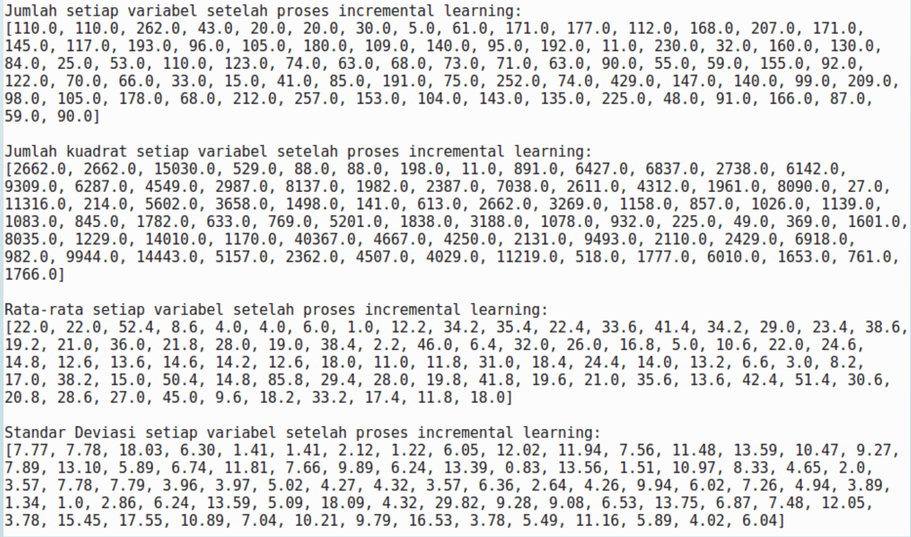
Implementasi Proses Incremental Learning



```
Jumlah setiap variabel sebelum proses incremental learning:
[88.0, 88.0, 210.0, 39.0, 16.0, 16.0, 24.0, 5.0, 51.0, 137.0, 143.0, 90.0, 136.0, 167.0, 140.0, 117.0,
95.0, 155.0, 78.0, 84.0, 146.0, 89.0, 112.0, 77.0, 160.0, 9.0, 186.0, 26.0, 128.0, 104.0, 68.0, 21.0,
45.0, 88.0, 99.0, 60.0, 51.0, 54.0, 59.0, 57.0, 51.0, 7z2.0, 45.0, 47.0, 125.0, 74.0, 98.0, 56.0, 54.0,
27.0, 13.0, 33.0, 69.0, 158.0, 61.0, 202.0, 60.0, 348.0, 119.0, 114.0, 82.0, 169.0, 78.0, 85.0, 144.0,
56.0, 172.0, 209.0, 123.0, 86.0, 120.0, 110.0, 183.0, 40.0, 73.0, 134.0, 71.0, 47.0, 72.0]

Jumlah kuadrat setiap variabel sebelum proses incremental learning:
[2178.0, 2178.0, 12326.0, 513.0, 72.0, 72.0, 162.0, 11.0, 791.0, 5271.0, 5681.0, 2254.0, 5118.0,
7709.0, 5326.0, 3765.0, 2503.0, 6693.0, 1658.0, 1946.0, 5882.0, 2211.0, 3528.0, 1637.0, 7066.0, 23.0,
9380.0, 178.0, 4578.0, 2982.0, 1242.0, 125.0, 549.0, 2178.0, 2693.0, 962.0, 713.0, 830.0, 943.0, 887.0,
701.0, 1458.0, 533.0, 625.0, 4301.0, 1514.0, 2612.0, 882.0, 788.0, 189.0, 45.0, 305.0, 1345.0, 6946.0,
1033.0, 11510.0, 974.0, 33806.0, 3883.0, 3574.0, 1842.0, 7893.0, 1710.0, 2029.0, 5762.0, 838.0, 8344.0,
12139.0, 4257.0, 2038.0, 3978.0, 3404.0, 9455.0, 454.0, 1453.0, 4986.0, 1397.0, 617.0, 1442.0]

Rata-rata setiap variabel sebelum proses incremental learning:
[22.0, 22.0, 52.5, 9.75, 4.0, 4.0, 6.0, 1.25, 12.75, 34.25, 35.75, 22.5, 34.0, 41.75, 35.0, 29.25,
23.75, 38.75, 19.5, 21.0, 36.5, 22.25, 28.0, 19.25, 40.0, 2.25, 46.5, 6.5, 32.0, 26.0, 17.0, 5.25,
11.25, 22.0, 24.75, 15.0, 12.75, 13.5, 14.75, 14.25, 12.75, 18.0, 11.25, 11.75, 31.25, 18.5, 24.5,
14.0, 13.5, 6.75, 3.25, 8.25, 17.25, 39.5, 15.25, 50.5, 15.0, 87.0, 29.75, 28.5, 20.5, 42.25, 19.5,
21.25, 36.0, 14.0, 43.0, 52.25, 30.75, 21.5, 30.0, 27.5, 45.75, 10.0, 18.25, 33.5, 17.75, 11.75, 18.0]

Standar Deviasi setiap variabel sebelum proses incremental learning:
[8.98, 8.98, 20.82, 6.65, 1.63, 1.63, 2.44, 1.25, 6.84, 13.88, 13.76, 8.73, 12.83, 15.67, 11.91, 10.68,
9.06, 15.12, 6.75, 7.78, 13.57, 8.77, 11.43, 7.18, 14.89, 0.95, 15.60, 1.73, 12.67, 9.62, 5.35, 2.21,
3.77, 8.98, 8.99, 4.54, 4.57, 5.80, 4.92, 4.99, 4.11, 7.34, 2.98, 4.92, 11.47, 6.95, 8.38, 5.71, 4.43,
1.5, 0.95, 3.30, 7.18, 15.32, 5.85, 20.88, 4.96, 34.30, 10.68, 10.40, 7.32, 15.84, 7.93, 8.61, 13.88,
4.24, 17.77, 20.18, 12.57, 7.93, 11.22, 11.23, 18.99, 4.24, 6.34, 12.87, 6.75, 4.64, 6.97]
```

Model sebelum incremental learning

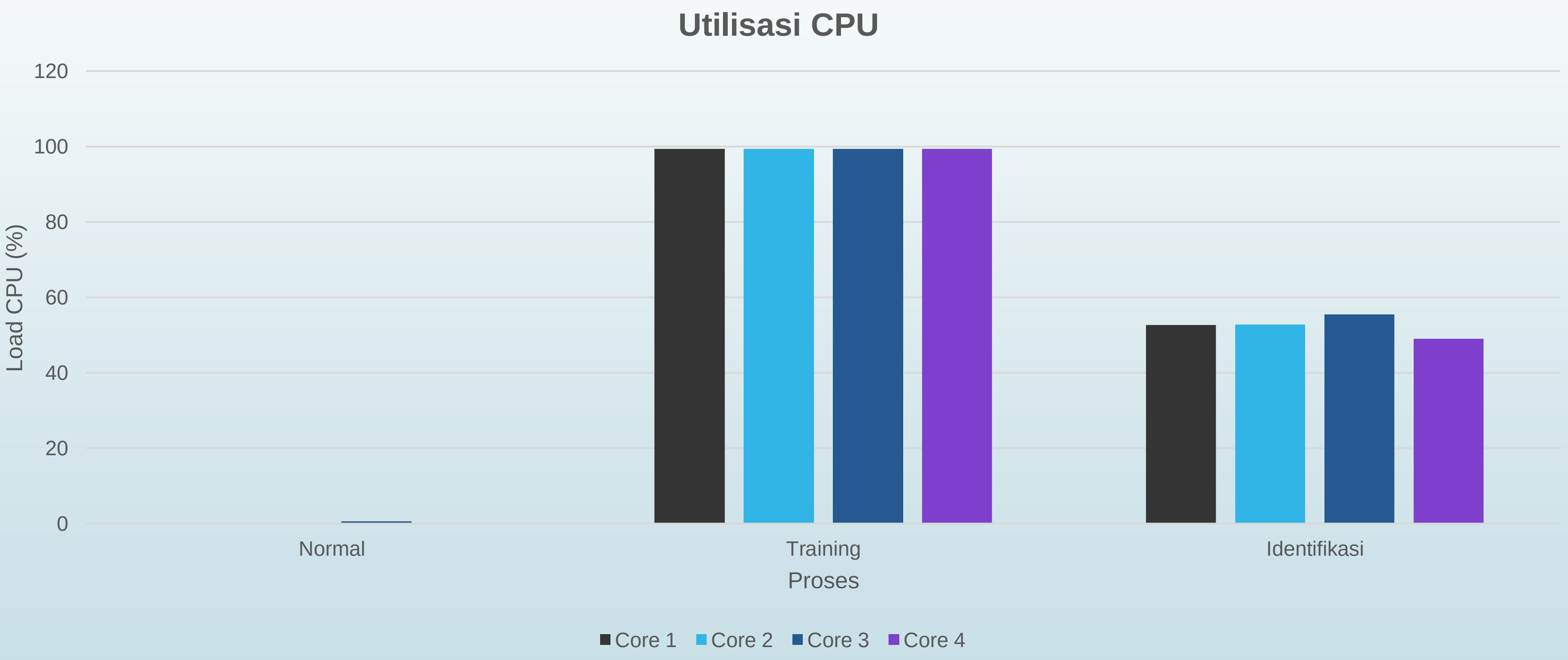
Model setelah incremental learning



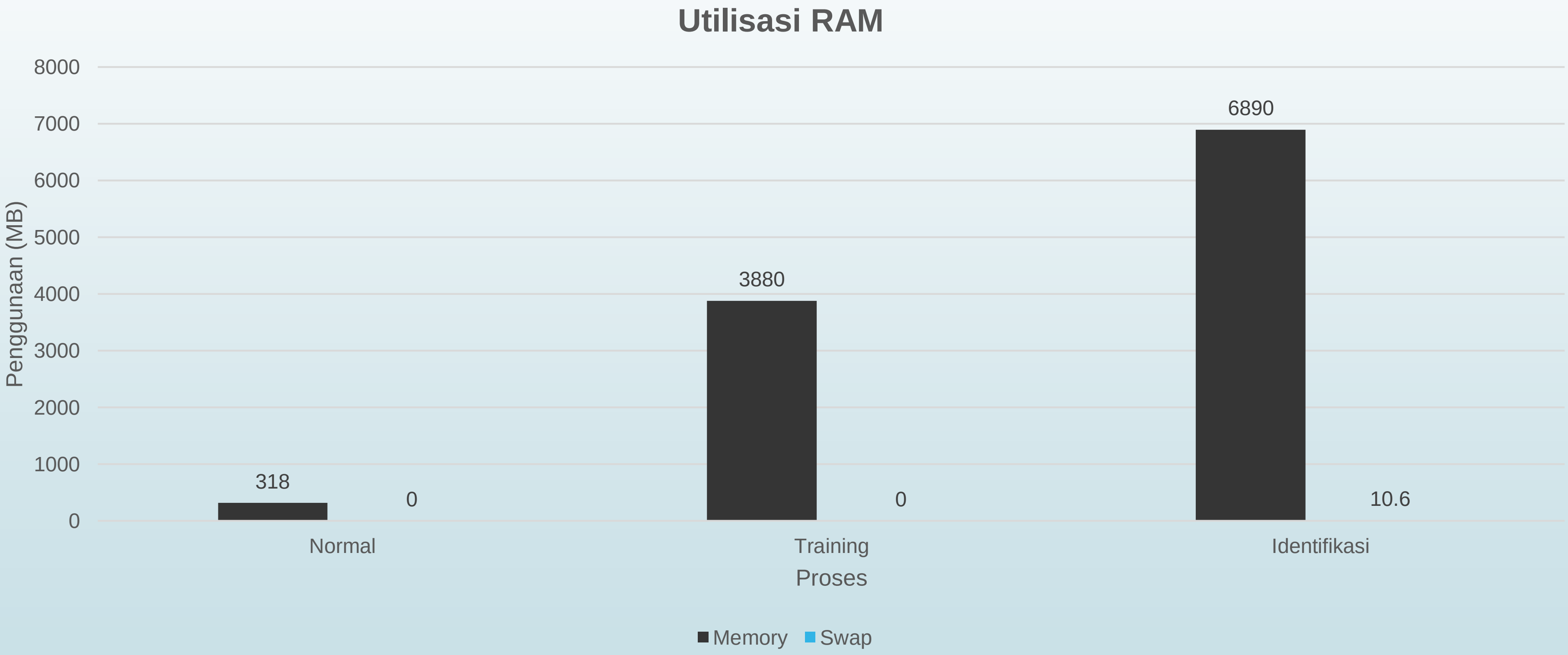
```
Jumlah setiap variabel setelah proses incremental learning:
[110.0, 110.0, 262.0, 43.0, 20.0, 20.0, 30.0, 5.0, 61.0, 171.0, 177.0, 112.0, 168.0, 207.0, 171.0,
145.0, 117.0, 193.0, 96.0, 105.0, 180.0, 109.0, 140.0, 95.0, 192.0, 11.0, 230.0, 32.0, 160.0, 130.0,
84.0, 25.0, 53.0, 110.0, 123.0, 74.0, 63.0, 68.0, 73.0, 71.0, 63.0, 90.0, 55.0, 59.0, 155.0, 92.0,
122.0, 70.0, 66.0, 33.0, 15.0, 41.0, 85.0, 191.0, 75.0, 252.0, 74.0, 429.0, 147.0, 140.0, 99.0, 209.0,
98.0, 105.0, 178.0, 68.0, 212.0, 257.0, 153.0, 104.0, 143.0, 135.0, 225.0, 48.0, 91.0, 166.0, 87.0,
59.0, 90.0]

Jumlah kuadrat setiap variabel setelah proses incremental learning:
[2662.0, 2662.0, 15030.0, 529.0, 88.0, 88.0, 198.0, 11.0, 891.0, 6427.0, 6837.0, 2738.0, 6142.0,
9309.0, 6287.0, 4549.0, 2987.0, 8137.0, 1982.0, 2387.0, 7038.0, 2611.0, 4312.0, 1961.0, 8090.0, 27.0,
11316.0, 214.0, 5602.0, 3658.0, 1498.0, 141.0, 613.0, 2662.0, 3269.0, 1158.0, 857.0, 1026.0, 1139.0,
1083.0, 845.0, 1782.0, 633.0, 769.0, 5201.0, 1838.0, 3188.0, 1078.0, 932.0, 225.0, 49.0, 369.0, 1601.0,
8035.0, 1229.0, 14010.0, 1170.0, 40367.0, 4667.0, 4250.0, 2131.0, 9493.0, 2110.0, 2429.0, 6918.0,
982.0, 9944.0, 14443.0, 5157.0, 2362.0, 4507.0, 4029.0, 11219.0, 518.0, 1777.0, 6010.0, 1653.0, 761.0,
1766.0]

Rata-rata setiap variabel setelah proses incremental learning:
[22.0, 22.0, 52.4, 8.6, 4.0, 4.0, 6.0, 1.0, 12.2, 34.2, 35.4, 22.4, 33.6, 41.4, 34.2, 29.0, 23.4, 38.6,
19.2, 21.0, 36.0, 21.8, 28.0, 19.0, 38.4, 2.2, 46.0, 6.4, 32.0, 26.0, 16.8, 5.0, 10.6, 22.0, 24.6,
14.8, 12.6, 13.6, 14.6, 14.2, 12.6, 18.0, 11.0, 11.8, 31.0, 18.4, 24.4, 14.0, 13.2, 6.6, 3.0, 8.2,
17.0, 38.2, 15.0, 50.4, 14.8, 85.8, 29.4, 28.0, 19.8, 41.8, 19.6, 21.0, 35.6, 13.6, 42.4, 51.4, 30.6,
20.8, 28.6, 27.0, 45.0, 9.6, 18.2, 33.2, 17.4, 11.8, 18.0]

Standar Deviasi setiap variabel setelah proses incremental learning:
[7.77, 7.78, 18.03, 6.30, 1.41, 1.41, 2.12, 1.22, 6.05, 12.02, 11.94, 7.56, 11.48, 13.59, 10.47, 9.27,
7.89, 13.10, 5.89, 6.74, 11.81, 7.66, 9.89, 6.24, 13.39, 0.83, 13.56, 1.51, 10.97, 8.33, 4.65, 2.0,
3.57, 7.78, 7.79, 3.96, 3.97, 5.02, 4.27, 4.32, 3.57, 6.36, 2.64, 4.26, 9.94, 6.02, 7.26, 4.94, 3.89,
1.34, 1.0, 2.86, 6.24, 13.59, 5.09, 18.09, 4.32, 29.82, 9.28, 9.08, 6.53, 13.75, 6.87, 7.48, 12.05,
3.78, 15.45, 17.55, 10.89, 7.04, 10.21, 9.79, 16.53, 3.78, 5.49, 11.16, 5.89, 4.02, 6.04]
```

PENGUJIAN DAN EVALUASI

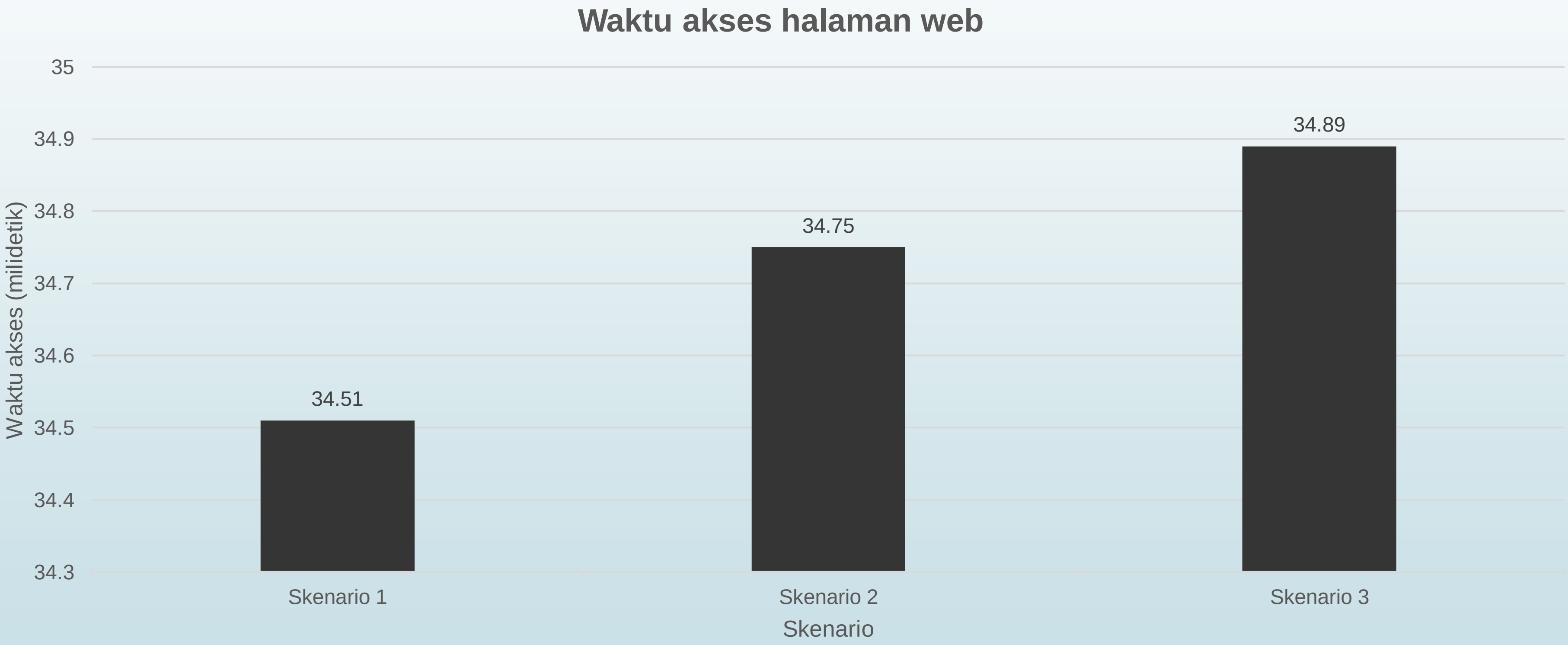
Uji Coba Performa



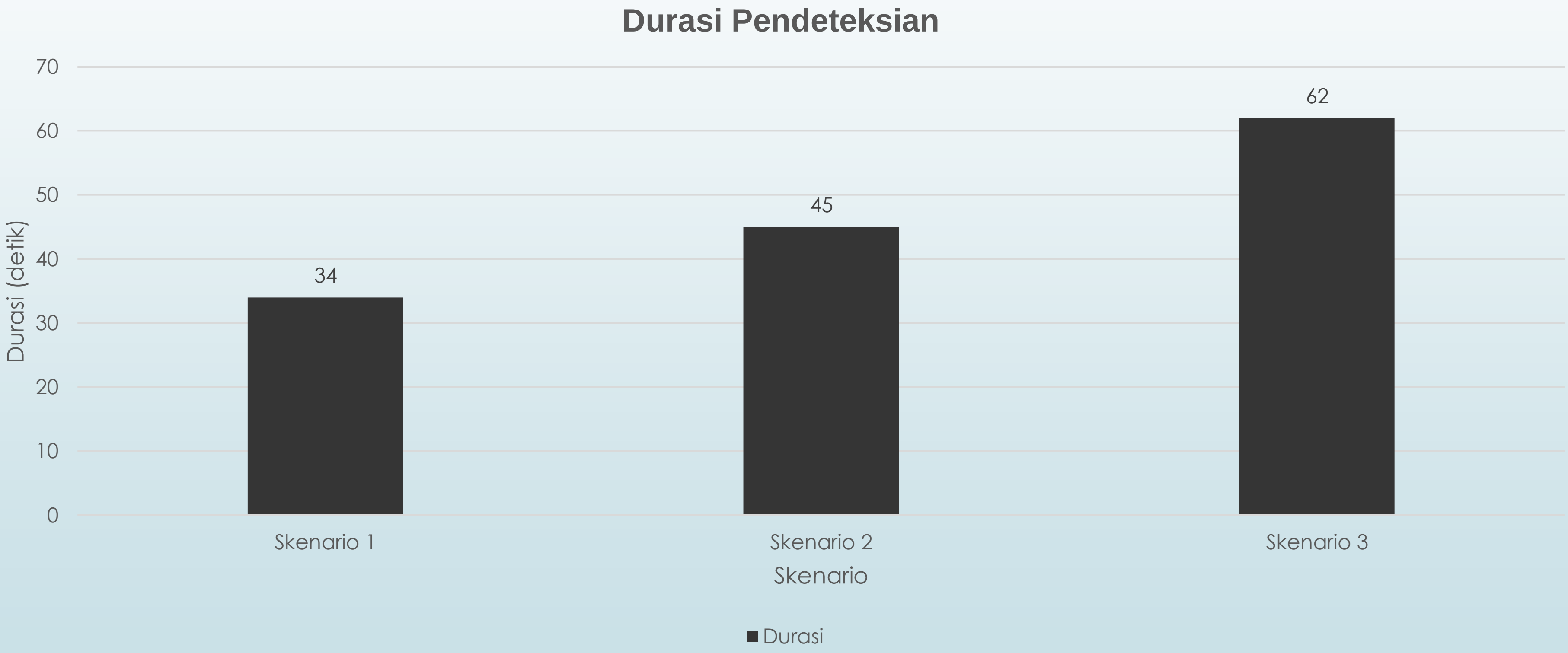
Uji Coba Performa (2)



Uji Coba Performa (3)



Uji Coba Kecepatan



Uji Coba Akurasi

Tabel Hasil Uji Data *Training* minimum jarak paket data intrusi

No	Window size	Jarak Port TCP				Jarak Port UDP
		21	23	25	80	53
1	10000	26.46	25.66	13.51	0.00	3.44
2	15000	26.46	22.52	13.51	0.00	5.41
3	20000	26.46	22.52	12.3	0.00	6.7

Tabel Threshold untuk masing-masing port

No	Threshold				
	Jarak Port TCP				Port UDP
	21	23	25	80	53
1	53.30	25.79	219.49	0.00	128.52

Tabel Hasil Uji Data *Training* maksimum jarak paket data normal

No	Window size	Jarak Port TCP				Jarak Port UDP
		21	23	25	80	53
1	10000	80.13	0	426.68	0.00	156.91
2	15000	80.13	0	426.68	0.00	210.08
3	20000	80.13	29.06	426.68	0.00	253.59

Uji Coba Tanpa Proses Incremental Learning

Tabel *Confussion matrix* uji coba

No	Window size	Kelas			
		A	B	C	D
1	10000	6	355	14	4935
2	20000	15	552	22	7926

Tabel hasil Uji Data *Testing* minggu ke-5

No	Window size	Jumlah connection	Jumlah Paket normal	Jumlah Paket serangan
1	10000	5328	5308	20
2	20000	8515	8478	37

Tabel hasil penilaian percobaan dengan ukuran window 10000

No	Jenis Penilaian	Nilai	Persentase
1	Akurasi (AC)	0.9307	93.07%
2	True positive rate (TP)	0.0166	1.66%
3	False negative rate (FN)	0.9834	98.34%
4	False positive rate (FP)	0.0028	0.28%
5	True negative rate (TN)	0.9972	99.72%
6	Presisi (P)	0.3	30.0%

Tabel hasil penilaian percobaan dengan ukuran window 20000

No	Jenis Penilaian	Nilai	Persentase
1	Akurasi (AC)	0.9324	93.26%
2	True positive rate (TP)	0.0265	2.65%
3	False negative rate (FN)	0.9375	97.35%
4	False positive rate (FP)	0.0028	0.28%
5	True negative rate (TN)	0.9972	99.82%
6	Presisi (P)	0.4054	40.54%

Uji Coba Dengan Proses Incremental Learning

Tabel *Confussion matrix* uji coba

No	Window size	Kelas			
		A	B	C	D
1	10000	187	174	3564	1403
2	20000	314	253	6397	1551

Tabel hasil Uji Data *Testing* minggu ke-5

No	Window size	Jumlah connection	Jumlah Paket normal	Jumlah Paket serangan
1	10000	5328	1577	3751
2	20000	8515	6711	1804

Tabel hasil penilaian percobaan dengan ukuran window 10000

No	Jenis Penilaian	Nilai	Persentase
1	Akurasi (AC)	0.2984	29.84%
2	True positive rate (TP)	0.518	51.58%
3	False negative rate (FN)	0.482	48.2%
4	False positive rate (FP)	0.7175	71.75%
5	True negative rate (TN)	0.2825	28.25%
6	Presisi (P)	0.0499	4.99%

Tabel hasil penilaian percobaan dengan ukuran window 20000

No	Jenis Penilaian	Nilai	Persentase
1	Akurasi (AC)	0.219	21.9%
2	True positive rate (TP)	0.5538	55.38%
3	False negative rate (FN)	0.4462	44.62%
4	False positive rate (FP)	0.8049	80.49%
5	True negative rate (TN)	0.1951	19.51%
6	Presisi (P)	0.0468	4.68%

KESIMPULAN DAN SARAN

Kesimpulan

1. Metode Mahalanobis *Distance* tidak dapat digunakan untuk mengklasifikasikan antara paket data normal dan paket data yang berupa intrusi untuk protokol HTTP. Jarak yang dihasilkan pada saat *training* menggunakan paket data normal maupun paket data yang berupa intrusi yaitu bernilai 0. Sehingga paket data normal maupun paket data intrusi tidak dapat dibedakan.
2. Sistem yang dibuat untuk pendeteksi intrusi menggunakan metode Mahalanobis *Distance* tanpa proses *incremental learning* dapat mendeteksi intrusi dengan persentase kebenaran sekitar 93%, namun dengan tambahan proses *incremental learning* hanya dapat mendeteksi intrusi dengan persentase kebenaran sekitar 20%. Dari hasil tersebut, dengan tambahan proses incremental learning mangurangi tingkat akurasi pendeteksian intrusi.

Saran

Adapun saran-saran yang diberikan untuk pengembangan sistem ini selanjutnya adalah karena membedakan paket data normal dengan paket data serangan menggunakan metode mahalanobis *distance* dengan proses *incremental learning* kurang akurat dibandingkan tanpa proses *incremental leraning*. Hal ini dikarenakan dengan menambahkan proses *incremental learning,* rata-rata dan standar deviasi pada model diperbaharui tetapi *threshold* yang digunakan untuk mendeteksi intrusi tidak diperbaharui, sehingga *threshold* yang ada tidak akurat untuk mendeteksi intrusi. Perlu ada implementasi metode lain sehingga dapat membantu meningkatkan keakuratan pendeteksian intrusi.

TERIMA KASIH