Suplemen Artikel “Deteksi Serangan Cyber Malware Berdasarkan Fitur Lalu Lintas Jaringan Menggunakan Neural Network”

1. Tabel Nama dan Deksripsi Fitur Dataset

|  |  |  |
| --- | --- | --- |
| **No** | **Nama Fitur** | **Deskripsi Fitur** |
| 1 | Source port | Port pengirim |
| 2 | Destination port | Port penerima |
| 3 | L3 / L4 Protocol identifier | Protokol yang dipakai pada layer 3 atau 4 |
| 4 | Flow Duration | Panjang durasi dari suatu flow network traffic |
| 5 | Total Forward Packets | Jumlah paket yang dikirimkan atau di-upload |
| ke luar dalam satu flow |
| 6 | Total Backward Packets | Jumlah paket yang diterima atau diunduh |
| 7 | Total Length of Forward Packets | Jumlah ukuran dari semua paket yang dikirim |
| dalam bentuk byte |
| 8 | Total Length of Backward | Jumlah ukuran dari semua paket yang |
| Packets | diterima dalam bentuk byte |
| 9 | Forward Packet Length Max | Ukuran maksimal atau ukuran terbesar dari |
| suatu paket yang dikirim |
| 10 | Forward Packet Length Min | Ukuran minimum atau ukuran terkecil dari |
| suatu paket yang dikirim |
| 11 | Forward Packet Length Mean | Rata-rata ukuran paket yang dikirim |
| 12 | Forward Packet Length Standard | Standar deviasi dari ukuran paket yang |
| Deviation | dikirim |
| 13 | Backward Packet Length Max | Ukuran maksimal atau ukuran terbesar dari |
| suatu paket yang diterima |
| 14 | Backward Packet Length Min | Ukuran minimum atau ukuran terkecil dari |
| suatu paket yang diterima |
| 15 | Backward Packet Length Mean | Rata-rata ukuran paket yang diterima |
| 16 | Backward Packet Length | Standar deviasi dari ukuran paket yang |
| Standard Deviation | diterima |
| 17 | Flow Byte/s | Jumlah byte yang dikirimkan dan diterima |
| setiap detiknya |
| 18 | Flow Packet/s | Jumlah paket yang dikirimkan dan diterima |
| setiap detiknya |
| 19 | Flow IAT(Inter-Arrival Time) Mean | Rata-rata waktu yang dibutuhkan dari satu pengiriman/penerimaan paket ke pengiriman/penerimaan paket yang |
| selanjutnya |
| 20 | Flow IAT Standar Deviation | Standar deviasi dari IAT antar paket |
| 21 | Flow IAT Max | Nilai IAT terbesar dalam satu flow |
| 22 | Flow IAT Min | Nilai IAT terkecil dalam satu flow |
| 23 | Forward IAT Total | Jumlah nilai IAT pada pengiriman paket |
| 24 | Forward IAT Mean | Rata-rata nilai IAT pada pengiriman paket |
| 25 | Forward IAT Standard Deviation | Standar deviasi dai nilai IAT pada pengiriman |
| paket |
| 26 | Forward IAT Max | Nilai IAT terbesar pada pengiriman paket |
| 27 | Forward IAT Min | Nilai IAT terkecil pada pengiriman paket |
| 28 | Backward IAT Total | Jumlah nilai IAT pada penerimaan paket |
| 29 | Backward IAT Mean | Rata-rata nilai IAT pada penerimaan paket |
| 30 | Backward IAT Standard | Standar deviasi dai nilai IAT pada penerimaan |
| Deviation | paket |
| 31 | Backward IAT Max | Nilai IAT terbesar pada penerimaan paket |
| 32 | Backward IAT Min | Nilai IAT terkecil pada penerimaan paket |
| 33 | Forward PSH(PUSH) Flag | Jumlah Flag PSH yang disertakan pada paket |
| yang dikirimkan |
| 34 | Backward PSH(PUSH) Flag | Jumlah Flag PSH yang disertakan pada paket |
| yang diterima |
| 35 | Forward URG(URGENT) Flag | Jumlah Flag URG yang disertakan pada paket |
| yang dikirimkan |
| 36 | Backward URG(URGENT) | Jumlah Flag URG yang disertakan pada paket |
| Flag | yang diterima |
| 37 | Forward Header Length | Total ukuran atau panjang dari header paket |
| yang dikirimkan |
| 38 | Backward Header Length | Total ukuran atau panjang dari header paket |
| yang diterima |
| 39 | Forward Packets/s | Jumlah paket yang dikirimkan setiap detiknya |
| 40 | Backward Packets/s | Jumlah paket yang diterima setiap detiknya |
| 41 | Min Packet Length | Ukuran paket terkecil |
| 42 | Max Packet Length | Ukuran paket terbesar |
| 43 | Packet Length Mean | Rata-rata ukuran paket |
| 44 | Packet Length Standard | Standar deviasi dari ukuran paket |
| Deviation |
| 45 | Packet Length Variance | Variasi dari ukuran paket |
| 46 | FIN Flag Count | Jumlah FIN Flag yang disertakan pada paket |
| yang dikirim atau diterima |
| 47 | SYN Flag Count | Jumlah SYN Flag yang disertakan pada paket |
| yang dikirim atau diterima |
| 48 | RST Flag Count | Jumlah RST Flag yang disertakan pada paket |
| yang dikirim atau diterima |
| 49 | PSH Flag Count | Jumlah PSH Flag yang disertakan pada paket |
| yang dikirim atau diterima |
| 50 | ACK Flag Count | Jumlah ACK Flag yang disertakan pada paket |
| yang dikirim atau diterima |
| 51 | URG Flag Count | Jumlah URG Flag yang disertakan pada paket |
| yang dikirim atau diterima |
| 52 | CWE Flag Count | Jumlah CWE Flag yang disertakan pada paket |
| yang dikirim atau diterima |
| 53 | ECE Flag Count | Jumlah ECE Flag yang disertakan pada paket |
| yang dikirim atau diterima |
| 54 | Down/Up Ratio | Perbandingan ukuran byte yang diunduh |
| dengan yang dikirimkan |
| 55 | Average Packet Size | Rata-rata ukuran paket yang dikirim dan |
| diterima |
| 56 | Average Forward Segment Size | Ukuran rata-rata yang diamati dalam arah |
| mengirim atau maju |
| 57 | Average Backward Segment | Ukuran rata-rata yang diamati dalam arah |
| Size | menerima atau mundur |
| 58 | Forward Average Bytes/Bulk | Jumlah rata-rata dalam ukuran besar byte |
| dalam arah maju |
| 59 | Forward Average Packets/Bulk | Jumlah rata-rata dalam ukuran besar paket |
| dalam arah maju |
| 60 | Forward Average Bulk Rate | Jumlah rata-rata dalam ukuran besar dengan |
| arah maju |
| 61 | Backward Average Bytes/Bulk | Jumlah rata-rata dalam ukuran besar byte |
| dalam arah mundur |
| 62 | Backward Average Packets/Bulk | Jumlah rata-rata dalam ukuran besar paket |
| dalam arah mundur |
| 63 | Backward Average Bulk Rate | Jumlah rata-rata dalam ukuran besar dengan |
| arah mundur |
| 64 | Sub Flow Forward Packets | Rata-rata jumlah paket pada sub flow dalam |
| arah maju atau mengirim |
| 65 | Sub Flow Forward Bytes | Rata-rata jumlah byte pada sub flow dalam |
| arah maju atau mengirim |
| 66 | Sub Flow Backward Packets | Rata-rata jumlah paket pada sub flow dalam |
| arah mundur atau menerima |
| 67 | Sub Flow Backward Bytes | Rata-rata jumlah byte pada sub flow dalam |
| arah mundur atau menerima |
| 68 | Init Win Bytes Forward | Jumlah bytes yang dikirimkan pada |
| inisialisasi window pada arah forward |
| 69 | Init Win Bytes Backward | Jumlah bytes yang dikirimkan pada |
| inisialisasi window pada arah backward |
| 70 | Act Data Packet Forward | Jumlah paket dengan minimal 1 byte data |
| pada TCP data payload dalam arah forward |
| 71 | Min Segment Size Forward | Minimum ukuran segment dalam arah maju |
| 72 | Active Mean | Waktu rata-rata flow aktif sampai pada |
| kondisi idle |
| 73 | Active Standard Deviation | Standar deviasi dari waktu suatu flow sampai |
| pada kondisi idle |
| 74 | Active Max | Waktu maksimum yang dibutuhkan suatu flow |
| sampai kondisi idle |
| 75 | Active Min | Waktu minimum suatu flow aktif sampai pada |
| kondisi idle |
| 76 | Idle Mean | Rata-rata waktu idle sampai pada kondisi |
| aktif |
| 77 | Idle Standard Deviation | Standar deviasi dari waktu idle sampai pada |
| kondisi aktif |
| 78 | Idle Max | Waktu maksimum suatu flow dalam kondisi |
| idle sampai pada kondisi aktif kembali |
| 79 | Idle Min | Waktu minimum suatu flow dalam kondisi |
| idle sampai pada kondisi aktif kembali |

1. Tabel Hasil Pengujian Fitur Studi Literatur

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | **Result** | | |
| **Hidden Neuron** | **Learning Rate** | **Epoch** | **Presisi** | **Recall** | **F1 Score** |
|  |  | 100 | 66.33% | 40.17% | 0.5004 |
|  |  | 200 | 66.33% | 40.08% | 0.4997 |
|  | 0.1 | 300 | 66.44% | 39.84% | 0.4981 |
|  |  | 100 | 67.82% | 42.53% | 0.5228 |
| 4 |  | 200 | 69.23% | 42.84% | 0.5293 |
|  | 0.05 | 300 | 70.72% | 42.97% | 0.5346 |
|  |  | 100 | 72.68% | 33.60% | 0.4596 |
|  |  | 200 | 69.02% | 38.38% | 0.4933 |
|  | 0.01 | 300 | 69.66% | 38.04% | 0.4921 |
|  |  | 100 | 67.98% | 44.41% | 0.5373 |
|  |  | 200 | 48.51% | 93.09% | 0.6379 |
|  | 0.1 | 300 | 48.55% | 93.10% | 0.6382 |
|  |  | 100 | 67.25% | 44.21% | 0.5335 |
| 5 |  | 200 | 69.01% | 43.61% | 0.5344 |
|  | 0.05 | 300 | 69.71% | 43.01% | 0.532 |
|  |  | 100 | 69.83% | 41.57% | 0.5212 |
|  |  | 200 | 70.18% | 42.76% | 0.5314 |
|  | 0.01 | 300 | 70.93% | 42.53% | 0.5318 |
|  |  | 100 | 59.20% | 52.16% | 0.5546 |
|  |  | 200 | 61.18% | 50.63% | 0.5541 |
|  | 0.1 | 300 | 63.45% | 49.51% | 0.5562 |
|  |  | 100 | 67.73% | 43.94% | 0.533 |
| 6 |  | 200 | 67.76% | 44.41% | 0.5366 |
|  | 0.05 | 300 | 67.82% | 44.89% | 0.5402 |
|  |  | 100 | 70.78% | 40.98% | 0.5191 |
|  |  | 200 | 71.53% | 42.07% | 0.5298 |
|  | 0.01 | 300 | 72.75% | 41.79% | 0.5308 |
|  |  | 100 | 47.34% | 98.07% | 0.6386 |
|  |  | 200 | 47.44% | 98.14% | 0.6396 |
|  | 0.1 | **300** | **47.58%** | **97.88%** | **0.6404** |
|  |  | 100 | 63.83% | 49.85% | 0.5598 |
| 12 |  | 200 | 64.46% | 49.78% | 0.5618 |
|  | 0.05 | 300 | 65.30% | 49.75% | 0.5648 |
|  |  | 100 | 70.69% | 42.65% | 0.532 |
|  |  | 200 | 71.30% | 42.57% | 0.5331 |
|  | 0.01 | 300 | 71.68% | 42.38% | 0.5326 |

1. Tabel Hasil Pengujian Fitur dari Peneliti

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | **Result** | | |
| **Hidden Neuron** | **LearningRate** | **Epoch** | **Presisi** | **Recall** | **F1 Score** |
|  |  | 100 | 52.04% | 83.05% | 0.6398 |
|  |  | 200 | 51.98% | 83.92% | 0.6419 |
|  | 0.1 | 300 | 51.34% | 84.29% | 0.6381 |
|  |  | 100 | 53.90% | 79.23% | 0.6415 |
| 4 |  | 200 | 54.29% | 78.71% | 0.6426 |
|  | 0.05 | 300 | 54.28% | 78.58% | 0.6421 |
|  |  | 100 | 68.54% | 30.81% | 0.4251 |
|  |  | 200 | 70.39% | 28.80% | 0.4088 |
|  | 0.01 | 300 | 73.62% | 28.77% | 0.4137 |
|  |  | 100 | 0.00% | 0.00% | 0 |
|  |  | 200 | 0.00% | 0.00% | 0 |
|  | 0.1 | 300 | 0.00% | 0.00% | 0 |
|  |  | 100 | 55.59% | 78.87% | 0.6521 |
| 5 |  | 200 | 55.84% | 79.06% | 0.6545 |
|  | 0.05 | 300 | 55.89% | 79.04% | 0.6547 |
|  |  | 100 | 71.97% | 28.39% | 0.4071 |
|  |  | 200 | 72.02% | 28.16% | 0.4049 |
|  | 0.01 | 300 | 71.97% | 28.10% | 0.4042 |
|  |  | 100 | 0.00% | 0.00% | 0 |
|  |  | 200 | 0.00% | 0.00% | 0 |
|  | 0.1 | 300 | 0.00% | 0.00% | 0 |
|  |  | 100 | 55.75% | 78.85% | 0.6531 |
| 6 |  | 200 | 55.88% | 79.05% | 0.6548 |
|  | 0.05 | 300 | 55.90% | 78.67% | 0.6536 |
|  |  | 100 | 70.60% | 25.89% | 0.3788 |
|  |  | 200 | 71.06% | 25.79% | 0.3785 |
|  | 0.01 | 300 | 71.39% | 25.78% | 0.3788 |
|  |  | 100 | 0.00% | 0.00% | 0 |
|  |  | 200 | 0.00% | 0.00% | 0 |
|  | 0.1 | 300 | 0.00% | 0.00% | 0 |
|  |  | 100 | 53.93% | 85.13% | 0.6603 |
| 12 |  | 200 | 54.94% | 83.45% | 0.6626 |
|  | 0.05 | **300** | **55.89%** | **82.39%** | **0.6660** |
|  |  | 100 | 0.00% | 0.00% | 0 |
|  |  | 200 | 0.00% | 0.00% | 0 |
|  | 0.01 | 300 | 0.00% | 0.00% | 0 |