P-ISSN : 1858-3938
E-ISSN : 2721-284X

Deteksi DDoS dengan *One Class Classification*

Oky Rahmanto
Program Studi Teknologi Informasi Politeknik Negeri Tanah Laut, Tanah Laut
E-mail : oky.rahmanto@politala.ac.id

Abstrak

Penggunaan teknik One-Class Classification telah lama digunakan untuk beberapa kasus dengan pengenalan pola dimana terdapat ketidakseimbangan data training antara 1 dengan lainnya. Kebanyakan dataset DDoS yang tersedia termasuk dalam hal ini. Penelitian ini bertujuan untuk melihat sejauh mana hasil training dengan teknik One Class Classification untuk mendeteksi adanya paket data berjenis serangan DDoS. Teknik One Class Classification yang digunakan dalam penelitian ini adalah One Class Support Vector Machine (OSVM). Perlakukan dataset pada fase Pra-proses sangat menentukan hasil dimana propertis dataset yang tersedia didalamnya terdapat data beerjenis kategori. *Training* dilakukan dengan pengaturan parameter nu dan gamma. Penentuan hasil secara keseluruhan menggunakan metrik f1-score. Nilai f1-score terendah pada pengaturan nu=0,075 dan gamma=1 dengan nilai 0.39615 Nilai f1-score tertinggi terdapat pada pengaturan parameter nu=0.025 dan gamma=1e-06 dengan nilai 0.97969.
Kata kunci: DDoS, OSVM, One Class Classification

Abstract

The use of the One-Class Classification technique has long been used for several cases with pattern recognition where there is an imbalance of training data between one and another. Most available DDoS datasets fall into this. This study aims to see how far the results of training with the One Class Classification technique are to detect the presence of DDoS attack-type data packets. One Class Classification technique used in this research is One Class Support Vector Machine (OSVM). Treating the dataset in the Pre-processing phase will determine the results where the available dataset properties include data of various categories. Training is done by setting the parameters nu and gamma. Determination of the overall results using the f1-score metric. The lowest f1-score value is at settings nu=0.075 and gamma=1 with a value of 0.39615 The highest f1-score value is found in parameter settings nu=0.025 and gamma=1e-06 with a value of 0.97969.
***Keywords**: DDoS, OSVM, One Class Classification*

1. Pendahuluan

DDoS adalah jenis serangan *Denial-of-Service* (DoS) memiliki karakteristik serangan dengan membanjiri server korban dengan paket data yang berasal dari server/mesin yang telah diretas sebelumnya(Agrawal & Tapaswi, 2019). Seluruh server/mesin yang telah diretas —disebut juga sebagai *bot*— akan mengirimkan paket data menuju target dalam rentang waktu bersamaan sehingga menghilangkan kemampuan target dalam memberikan pelayanan terhadap pengguna yang sebenarnya.

Salah satu bentuk mesin yang dapat diretas dan menjadi *bot* dalam serangan DDoS tersebut adalah perangkat *Internet of Things* dikarenakan memiliki kemampuan dalam melakukan akses terhadap jaringan serta mengirimkan paket data serta kurangnya pertahanan dan kontrol akses di banyak perangkat *Internet of Things* (IoT)(Zhang dkk., 2020). Selain itu, dengan terus meningkatnya penggunaan perangkat IoT, maka secara tidak langsung akan menjadi faktor dalam bertambahnya jenis serta volume dari *bot* yang dapat melakukan serangan.

Setiap terjadi serangan DDoS, perlu dilakukan tindakan preventif dalam berbagai aspek keamanan agar layanan server dapat berjalan normal tanpa terpengaruh serangan yang terjadi. Sehingga diperlukan adanya mekanisme deteksi dalam hal membedakan antara paket data normal dan paket data serangan. Salah satu cara untuk melakukan pemisahan antara paket data normal dan paket data serangan adalah dengan mengunakan teknik *Pattern Matching and Fingerprinting (Agrawal & Tapaswi, 2019)*, yaitu Metode pendeteksian berdasarkan kemiripan paket data didalam jaringan (Chonka dkk., 2009). Mekanisme bekerja dengan cara mempelajari pola paket data serangan DDoS pada masa lampau sehingga menemukan bentuk pola yang disebut sebagai model untuk melakukan prediksi klasifikasi untuk paket data yang terbaru.

Model klasifikasi ini akan membedakan antara paket data normal dengan paket data serangan DDoS dengan cukup baik selama data paket masa lampau cukup dan seimbang dalam ketika melakukan pembentukan pola pada saat *training* model dilakukan. namun dalam

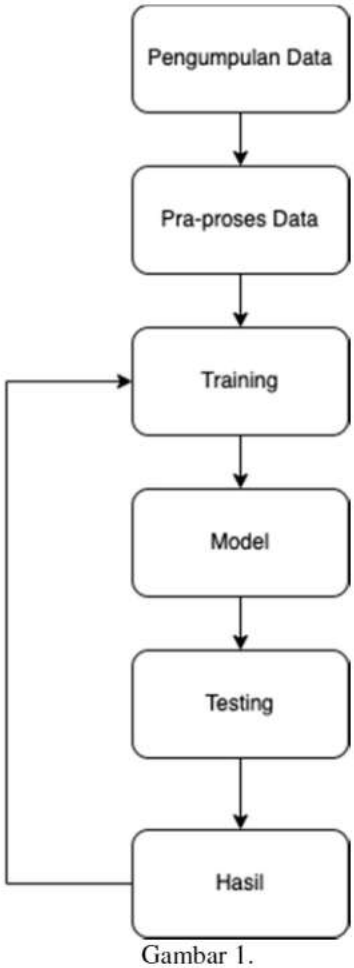
P-ISSN : 2502-3357
E-ISSN : 2721-284X

kenyataannya, seringkali jumlah paket data yang tersedia untuk dilakukan pembelajaran tidak dalam bentuk seimbang dimana jenis paket serangan DDoS lebih besar dibandingkan paket data normal.

Salah satu teknik pembelajaran yang dapat digunakan dalam penggunakan data tidak seimbang adalah *One Class Classification*. Menurut (Khan & Madden, 2014), pendekatan *One Class Classification* (OCC) biasanya diterapkan pada bidang klasifikasi teks, pengenalan angka tulisan tangan, pengenalan wajah, analisis medis, bioinformatika, deteksi spam, serta pendeteksian anomaly. Kemampuan One Class Classification dalam melakukan pembelajaran tidak seimbang akan sangat membantu pembentukan model pembelajaran paket data serangan DDoS.

2. Metode Penelitian

Berikut adalah penjabaran dari langkah-langkah penelitian yang dilakukan



Gambar 1.

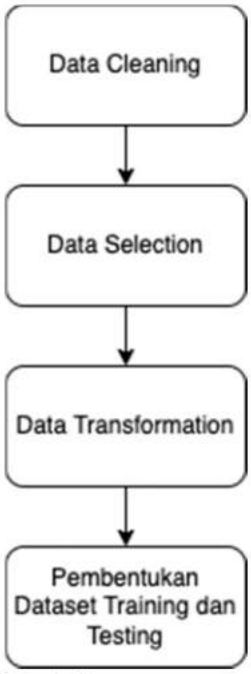
2.1. Pengumpulan data

Pada tahap ini, peneliti mendapatkan data berasal dari sumber terbuka *DDoS Botnet Attack on IOT Devices* tersedia pada https://www.kaggle.com/datasets/siddharthm1698/ddos-botnet-attack-on-iot-devices. Dataset ini berisi 47 kolom yang didalamnya beberapa propertis seperti *source port, source address, destination port, destination address* serta jumlah paket data yang merupakan bagian komponen penting dalam pendeteksian serangan DDoS

Pada proses training one class classification, hanya data positif yang diperlukan untuk, tetapi data pasien negatif juga diperlukan untuk fase evaluasi (pengujian). Data negatif yang dibutuhkan juga lebih sedikit karena hanya digunakan untuk pengujian.

2.2. Pra-Pemrosesan data

Pra-pemrosesan data dilakukan untuk memastikan data mentah telah siap untuk dimasukkan dalam *training* untuk *One-Class Classification*. Tahapan yang dilalui berupa *Data Cleaning, Data Integration, Data Transformation* serta pembentukan dataset training dan testing



Gambar 1. Langkah pra-pemrosesan data

A. Data Cleaning

Proses cleaning dilakukan dengan cara melakukan pengecekan terhadap data yang memiliki instance kosong serta menghapus instance tersebut.

B. Data Selection

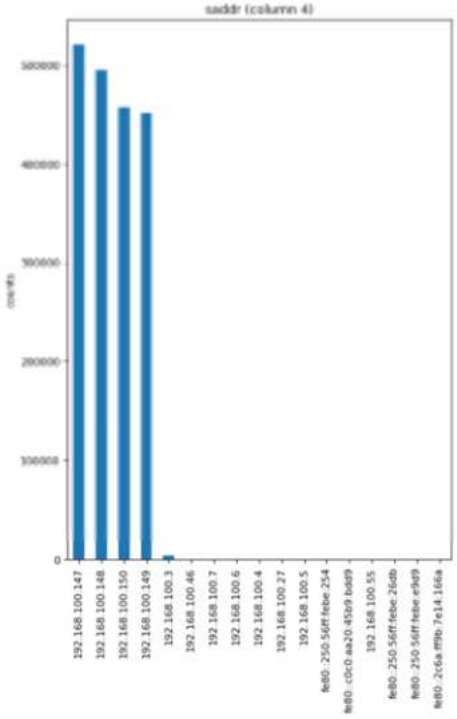
P-ISSN : 1858-3938
E-ISSN : 2721-284X

Proses ini dilakukan untuk memilih propertis dari data yang akan digunakan. Proses ini meilibatkan adanya *exploratory analysis* serta studi referensi dalam hal karakteristik paket data. Analisis dalam penelitian ini bertujuan untuk mengenal paket data yang berjenis serangan, dalam hal ini fokus pada penyerang sehingga propertis data yang dipilih berupa *protocol, source ip , source port, count_pkts, CountPktsStateDestIP, CountPktsStateSrcIP*.

C. Data Transformation

Umumnya prses *transformasi* data akan melakukan setiap propertis data menjadi nilai MinMax[0,1]. Namun dalam kasus DDoS, tidak semua propertis dapat menjadi nilai MinMax[0,1]. Berberapa propertis memiliki sifat cetgorical yang dimana diharuskan melakukan beberapa analisis sebelum ditransformasi menjadi MinMax[0,1].

Salah satu data yang diperlukan analisis terlebih dahulu adalah sourceIP dan sourcePort. Kedua propertis perlu dilakukan proses ranking berdasarkan frekuensi dari kemunculan data tersebut. Jika melihat dari *explanatory analysis* dengan menggunakan *distribution column*, terlihat ada 5 jenis source IP yang cukup besar frekuensi tersebut sehingga, data training akan diplih dari frekuensi tersebut. Untuk propertis data berupa *source port* juga dilakukan ranking dengan berdasarkan frekuensi karena data *source port* cukup tersebar merata.



Gambar 1. *Explanatory Analysis* menggunakan *Column Distribution* untuk *Source IP*

Selanjutnya dilakukan normalisasi MinMax[0,1] untuk setiap propertis data. Untuk data kategori protocol, normaliasi dilakukan dengan memberikan label [0,1] dikarenakan hanya terdapat 2 buah data yaitu [TCP,UDP]

D. Pembentukan dataset training dan testing

Dataset yang diperlukan dalam One Class Classification harus tidak seimbang, dalam hal ini untuk training menggunakan 41700 data DDoS serta 0 data normal. Untuk testing digunakan 417 data DDoS dan 417 data normal

Tabel 1. Distribusi data training dan testing

Jenis Data	Training	Testing
DDoS	41700	417
Normal	0	417

2.3. One Class SVM

Formulasi SVM pada umumnya memaksimalkan margin batas antara dua kelas data. Untuk *One Class SVM,* (Schölkopf dkk., 1999) mengubah SVM menjadi pencarian hyperplane menggunakan jarak pemisahan maksimum antara titik data yang diberikan (data positif) dan titik asal. Hasil training merupakan fungsi biner yang dapat memetakan apakah titik uji kemungkinan berada di dalam (positif) atau di luar (negatif) rentang data pelatihan. Formulasi *One Class SVM* ini memiliki parameter tambahan yang disebut ν (nu) dengan nilai antara 0 dan 1. Nilai ν menentukan batas maksimum pada proporsi outlier dalam kumpulan data pelatihan dan batas minimum pada jumlah proporsi vektor pendukung untuk kumpulan data pelatihan (Azkiya dkk., 2017).

Keakuratan metode *One Class SVM* dalam prediksi bergantung pada optimasi nilai parameter yang digunakan dalam penelitian. Parameternya adalah gamma dan nu. Nilai parameter gamma harus lebih besar dari 0, tetapi nilai parameter nu lebih kecil dari 1. Untuk mendapatkan nilai akurasi terbaik, diperlukan beberapa pengaturan parameter. Langkah-langkah yang dilakukan adalah pelatihan *One Class SVM* dan pengujian *One Class SVM*. Pelatihan *One Class SVM* menggunakan set data pelatihan dengan nilai gamma (γ) dan nu (ν) yang berbeda (Azkiya dkk., 2017).

3. Hasil Penelitian dan Pembahasan

Metrik yang digunakan untuk evaluasi adalah precision, recall, f-1 score, dan akurasi. Untuk penelitian ini, f-1 score menjadi acuan karena pada umumnya, deteksi ddos merupakan bagian dari mitigasi dari serangan. Pendeteksian ini akan membangkitkan *alarm system* untuk mengatur keputusan sebuah paket data yang sedang masuk dan harus dapat diidentifikasi dengan tepat. Jika terdeteksi DDoS, maka paket data akan dilakukan

P-ISSN : 2502-3357
E-ISSN : 2721-284X

drop packet, jika merupakan paket normal, maka paket data akan diteruskan

Dalam penggunaan metrik pada penelitian ini. TP/True Positif adalah hasil paket data yang teridentifikasi benar sebagai DDoS. TN/ True Negatif adalah paket data yang

$$p = \frac{TP}{TP + FP} \quad (2)$$

$$r = \frac{TP}{TP + FN} \quad (1)$$

Tabel 2. Hasil pengujian menggunakan metrik *Precision*

ν \ γ	1	0.1	0.01	0.001	0.0001	1e-05	1e-06
0.025	1.0	0.99278	0.8139	0.7135	0.70475	0.84124	0.97619
0.05	1.0	0.99301	0.81572	0.7197	0.74952	0.97821	0.97525
0.075	1.0	0.99213	0.81707	0.72921	0.79789	0.97767	0.98741
0.1	1.0	0.99251	0.82673	0.76605	0.83636	0.98219	0.98734
0.125	1.0	0.99291	0.83551	0.7679	0.86506	0.98128	0.98953
0.15	1.0	0.99245	0.84881	0.81567	0.91885	0.98066	0.98919
0.175	1.0	0.99262	0.87395	0.82118	0.99112	0.98844	0.99721
0.2	1.0	0.99278	0.87536	0.85459	0.99065	0.99157	0.99708

Tabel 3. Hasil pengujian menggunakan metrik *Accuracy*

ν \ γ	1	0.1	0.01	0.001	0.0001	1e-05	1e-06
0.025	0.71823	0.82734	0.80336	0.78058	0.77938	0.89688	0.97962
0.05	0.68345	0.83813	0.80815	0.77818	0.81055	0.97362	0.96043
0.075	0.6235	0.79976	0.81175	0.78417	0.83933	0.96163	0.96403
0.1	0.67146	0.81535	0.81655	0.80815	0.85492	0.95444	0.96163
0.125	0.70863	0.83333	0.80815	0.79616	0.86331	0.93165	0.94844
0.15	0.67986	0.81295	0.81535	0.82854	0.88369	0.91727	0.93405
0.175	0.69904	0.82014	0.82014	0.82734	0.89808	0.90528	0.92686
0.2	0.64388	0.82734	0.81055	0.83333	0.8777	0.91966	0.90767

Tabel 4. Hasil pengujian menggunakan metrik *Recall*

ν \ γ	1	0.1	0.01	0.001	0.0001	1e-05	1e-06
0.025	0.43645	0.65947	0.78657	0.93765	0.96163	0.97842	0.98321
0.05	0.36691	0.68106	0.79616	0.91127	0.93285	0.96882	0.94484
0.075	0.247	0.60432	0.80336	0.90408	0.90887	0.94484	0.94005

0.1	0.34293	0.63549	0.80096	0.88729	0.88249	0.92566	0.93525
0.125	0.41727	0.67146	0.76739	0.84892	0.86091	0.8801	0.90647
0.15	0.35971	0.6307	0.76739	0.84892	0.84173	0.85132	0.8777
0.175	0.39808	0.64508	0.7482	0.83693	0.80336	0.82014	0.85612
0.2	0.28777	0.65947	0.72422	0.80336	0.76259	0.84652	0.81775

Tabel 5. Hasil pengujian menggunakan teknik *F1-Score*

ν \ **γ**	**1**	**0.1**	**0.01**	**0.001**	**0.0001**	**1e-05**	**1e-06**
0.025	0.60768	0.79251	0.8	0.81036	0.81339	0.90466	0.97969
0.05	0.53684	0.80797	0.80583	0.80423	0.8312	0.97349	0.95981
0.075	0.39615	0.75112	0.81016	0.80728	0.84978	0.96098	0.96314
0.1	0.51071	0.77485	0.81364	0.82222	0.85881	0.95309	0.96059
0.125	0.58883	0.80114	0.8	0.80638	0.86298	0.92794	0.94618
0.15	0.5291	0.77126	0.80605	0.83196	0.8786	0.91142	0.93011
0.175	0.56947	0.78198	0.8062	0.82898	0.88742	0.89646	0.92129
0.2	0.44693	0.79251	0.79265	0.82818	0.86179	0.91332	0.89855

Nilai metrik yang terbaik adalah berupa > 0.9 dan < 1. Berada pada angka 1, maka model akan mengalami *overfitting*. Namun jika kurang dari angka 0.9, maka model tidak dapat melakukan klasifikasi dengan baik, sehingga perlu dilakukan perulangan dalam membangun model serta pengujian dengan nilai gamma dan nu yang bervariasi. Nilai nu = [0.025,0.05,0.075,0.1,0.125,0.15,0.175,0.2] serta nilai gamma =[1,0.1,0.01 0.001,0.0001,1e-05,1e-06].

Jika melihat dari nilai *precision* pada tabel 2, maka nilai tertinggi selalu didapat jika gamma = 1, hal ini menunjukkan jika menggunakan gamma=1 maka akan terjadi *overfitting,* yaitu kondisi dimana model yang dihasilkan dari training akan selalu tepat untuk hasil pola yang telah dipelajari namun tidak akurat untuk pola-pola yang sedikit berbeda dari data training. *Overfitting* ini dapat dideteksi dengan menggunakan metrik lainnya perlu yaitu *recall* dan *accuracy.* Nilai rerata *accuracy* terlihat paling rendah didapatkan jika *gamma*=1. Nilai *recall* untuk pada gamma=1 juga terlihat lebih rendah. Sehingga bisa diperkirakan untuk nilai gamma=1 maka model hasil training terjadi *overfitting*.

Metrik lainya untuk melihat hasil uji secara umum dengan cara melihat hasil dari perhitungan f1-score. Pada metrik f1-score terlihat hasil terendah pada pengaturan nu=0,075 dan gamma=1 dengan nilai 0.39615. Hasil tertinggi didapat dengan pengaturan parameter nu=0.025 dan gamma=1e-06 dengan nilai 0.97969.

4. Kesimpulan

Secara umum, teknik One Class Clasification dapat digunakan untuk mendeteksi serangan DDoS dengan mempelajari pola dari paket data serangan DDoS pada masa lampau. Namun data tersebut harus dilakukan pre-proses terlebih dahulu terutama pada propertis data berjenis kategori seperti *protocol, source IP dan source Port*. Hal ini disebabkan teknik One Class Clasisfication yang digunakan adalah SVM yang dimana membutukkan data dalam bentuk angka. Nilai parameter terbaik

5. Referensi

Agrawal, N., & Tapaswi, S. (2019). Defense Mechanisms Against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges. *IEEE Communications Surveys & Tutorials*, *21*(4), 3769–3795. https://doi.org/10.1109/COMST.2019.2934468

P-ISSN : 2502-3357
E-ISSN : 2721-284X

Azkiya, Z. Z., Indriani, F., & Chandra, H. K. (2017). Deteksi Penyakit Dengue Hemorrhagic Fever dengan Pendekatan One Class Classification. *Journal of Information Systems Engineering and Business Intelligence*, *3*(2), 129–133. https://doi.org/10.20473/jisebi.3.2.129-133

Chonka, A., Singh, J., & Zhou, W. (2009). Chaos theory based detection against network mimicking DDoS attacks. *IEEE Communications Letters*, *13*(9), 717–719. https://doi.org/10.1109/LCOMM.2009.090615

Khan, S. S., & Madden, M. G. (2014). One-class classification: Taxonomy of study and review of techniques. *The Knowledge Engineering Review*, *29*(3), 345–374. https://doi.org/10.1017/S026988891300043X

Schölkopf, B., Williamson, R. C., Smola, A., Shawe-Taylor, J., & Platt, J. (1999). Support Vector Method for Novelty Detection. *Advances in Neural Information Processing Systems*, *12*. https://papers.nips.cc/paper/1999/hash/8725fb777f25776ffa9076e44fcfd776-Abstract.html

Zhang, X., Upton, O., Beebe, N. L., & Choo, K.-K. R. (2020). IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers. *Forensic Science International: Digital Investigation*, *32*, 300926. https://doi.org/10.1016/j.fsidi.2020.300926