Jurnal Media Pratama
Volume 18 No. 1 Edisi: Juni 2024, Halaman: 39 - 45 e-ISSN: 2721-9690

Klasifikasi Tingkat Ancaman Siber menggunakan Pembelajaran Mesin pada Web Application Firewall (WAF)

Cyber threat level classification using machine learning on Web Application Firewall (WAF)

Mukhlis Prasetyo Aji[1*]
[1)]Program Studi Teknik Informatika, Fakultas Teknik dan Sains
Universitas Muhammadiyah Purwokerto
Jl. K.H. Ahmad Dahlan, Dukuhwaluh, Kembaran 53182, Indonesia
email: [*1]prasetyo-aji@ump.ac.id

ABSTRAK

Serangan siber yang terjadi semakin berkembang pesat hingga menyasar data pada sistem informasi di suatu organisasi. Salah satu data yang menjadi sasaran adalah data privasi pengguna sistem informasi tersebut. Untuk itu, penelitian bertujuan untuk mengatasi kekhawatiran adanya serangan tersebut dengan melakukan investigasi forensik digital terhadap pola kejahatan siber dengan menyiapkan analisis log Web Application Firewall (WAF) pada sistem di suatu organisasi. Penelitian ini menggunakan metode *LGBM Classifier*, k-Nearest Neighbors (KNN), Random Forest (RF) dan Decision Tree (DT Algorithm untuk mengidentifikasi dan mengklasifikasikan jenis serangan yang terjadi pada sistem informasi. Hasil percobaan yang telah dilakukan diperoleh data akurasi sebesar 96,63%.

Kata Kunci: Forensik Digital, Pembelajaran Mesin, Kumpulan Data, Firewall Aplikasi Web, Klasifikasi Serangan

(Dikirim: 20 Mei 2024, Direvisi: 25 Mei 2024, Diterima: 26 Mei 2024)

ABSTRACT

Cyber attacks that occur are growing rapidly enough to target data on information systems in organizations.One of the data that is targeted is the privacy data of users of the information system.For this reason, research aims to overcome the concerns of these attacks by conducting digital forensic investigations of cybercrime patterns by preparing Web Application Firewall (WAF) logs analysis on systems in organizations.This research uses the LGBM Classifier, k-Nearest Neighbors (KNN), Random Forest (RF) dan Decision Tree (DT Algorithm methods to identify and classify the types of attacks that occur on the information system. The results of the experiments that have been carried out obtained accuracy data of 96.63%.

Keywords: *Digital Forensics, Machine learning, Dataset, Web Application Firewal, Attack classification*

1. Pendahuluan

Ancaman keamanan dan serangan siber merupakan masalah utama yang menembus jaringan dan menyebabkan kerusakan mendadak pada akun keuangan dan bisnis dengan memengaruhi server [1]. Berbagai serangan pada jaringan terletak Internet Control Message Protocol Attack, Transmission Control Protocol Sync Attack, dan User Datagram Protocol Attack pada protocol jaringan dapat diklasifikasikan berdasarkan pembelajaran mesin [2]. Bahaya yang paling sering dilaporkan terhadap

keamanan komputer adalah malware. Metode klasifikasi malware sering kali diperlukan untuk memprioritaskan ini karena tim keamanan tidak dapat menangani semua malware tersebut sekaligus [3]. Deteksi dan klasifikasi ancaman jaringan berdasarkan pembelajaran mesin, yang merupakan bagian dari ancaman cerdas teknologi analisis ancaman cerdas [4]. Pada penelitian yang lain bahwa Analisis forensik botnet membantu dalam memahami sifat serangan dan modus operandi yang digunakan oleh para penyerang [5]. Beberapa teknik berbasis pembelajaran mesin telah dikembangkan dalam literatur untuk mengidentifikasi jenis Serangan keamanan siber yang menargetkan perangkat lunak [6].

Biro Sistem Informasi merupakan salah satu unit yang mengelola website dan server di Universitas Muhammadiyah Purwokerto, menghadapi tantangan terhadap keamanan. Teknik responsif standar, seperti antivirus, firewall, spyware, dan mekanisme otentikasi memberikan keamanan di banyak area tetapi masih menghadapi tantangan serangan intrusi dan virus. Sementara itu, untuk mengatasi mengatasi keterbatasan serangan intrusi dan virus, Intrusion Detection System (IDS) telah diusulkan oleh para peneliti sebelumnya menggunakan beberapa teknik Machine Learning (ML) Classifier tetapi juga memiliki beberapa kelemahan utama seperti berurusan dengan dataset lama sedikit jumlah kelas serangan, tidak dapat memonitor kelas serangan baru, alarm palsu yang tinggi dan sebagainya [7].

Dalam penelitian ini kami bertujuan untuk menganalisis dan mengklasifikasikan serangan yang terjadi dan menggunakan dataset Logs Web Application Firewall (WAF). Sedangkan algoritma yang digunakan peneliti menggunakan *LGBM Classifier*, k-Nearest Neighbors (KNN), Random Forest (RF) dan Decision Tree (DT) dengan bahasa pemrograman phyton.

2. Tinjauan Pustaka

2.1. *LGBM Classifier*

LGBM Classifier, yang umumnya disebut sebagai Light Gradient Boosting Machine Classifier, adalah model klasifikasi. *LGBM Classifier* menggunakan pendekatan pohon keputusan untuk tugas pembelajaran mesin seperti pemeringkatan dan klasifikasi. *LGBM Classifier* menggunakan pendekatan *Gradient-based One-Side Sampling* (GOSS) dan Exclusive Feature Bundling (EFB) untuk menangani data berskala besar secara efektif, meningkatkan kecepatan pemrosesan, dan meminimalkan penggunaan memori [8].

2.2. K Nearest Neighbors Classifier

Nearest Neighbors Classifier, juga disebut sebagai k-NN, adalah jenis algoritma pembelajaran mesin yang digunakan untuk regresi sampel dan klasifikasi. Ini adalah teknik yang diawasi dan non-parametrik. Sistem pengklasifikasi dibangun berdasarkan kesamaan antara vektor data baru dan lama. Sistem ini mempertahankan data selama fase pelatihan. Setelah penambahan kumpulan data baru, data tersebut diklasifikasikan ke dalam kategori yang paling mirip dengan data dalam kumpulan data asli. Dalam kumpulan data pengujian atau validasi, parameter k mengidentifikasi contoh-contoh yang menunjukkan tingkat kesamaan tertinggi dengan kelompok kasus tertentu. Untuk mengukur kesamaan antara dua titik, hitung jarak Euclidean dari pusat [9].

2.3. Pengklasifikasi Pohon Keputusan (DT)

Pengklasifikasi DT Pohon keputusan (DT) adalah model komputasi yang menggunakan struktur seperti pohon untuk membuat keputusan berdasarkan serangkaian kondisi dan hasil. Pohon keputusan (DT) adalah jenis algoritma yang digunakan dalam pembelajaran mesin dan penambangan data. Pohon keputusan (DT) adalah representasi grafis dari proses pengambilan keputusan, di mana setiap simpul mewakili keputusan atau pengujian pada atribut tertentu, dan setiap cabang mewakili Pohon Keputusan (DT) adalah jenis algoritma pembelajaran mesin terbimbing yang digunakan untuk tugas klasifikasi dan regresi [10]. Simpul keputusan dan simpul daun adalah dua jenis simpul berbeda yang menyusun pohon keputusan (DT). Simpul keputusan adalah entitas kompleks yang terdiri dari beberapa bagian, dan tujuannya adalah untuk

menghasilkan aturan untuk membuat keputusan. Sebaliknya, simpul daun mewakili hasil akhir yang berasal dari aturan keputusan dan tidak menghasilkan cabang tambahan. Kriteria keputusan dibangun berdasarkan atribut dari kumpulan data yang diberikan (1.1). Algoritma Klasifikasi dan Regresi (Algoritma CART) digunakan untuk membangun pohon. DT selanjutnya mengkategorikan cabang-cabang dengan memanfaatkan nilai benar (positif) atau salah (negatif) [11].

2.4. Pengklasifikasi Random Forest (RF)

Random Forest (RF) adalah algoritma pembelajaran mesin. RF, pengklasifikasi pembelajaran mesin yang diawasi, dapat secara efektif mengatasi masalah regresi dan klasifikasi. Pengklasifikasi Random Forest menggunakan banyak pohon keputusan pada berbagai subset informasi input, merata-ratakan hasilnya untuk meningkatkan akurasi [12].

3. Metode

Sebelum mendalami metode yang diusulkan, kami memperkenalkan pendekatan yang diusulkan secara singkat. Kami membagi alur kerja solusi yang diusulkan ke dalam lima langkah. Langkah pertama adalah Exploratory Data Analysis kemudian menerapkan teknik preprocessing yang sesuai pada langkah kedua. Pada langkah ketiga, menghitung bobot berdasarkan distribusi kelas (serangan). Setelah estimasi bobot, kami mengklasifikasikan sub-bagian menggunakan algoritma *LGBM Classifier*, *k-Nearest Neighbors* (KNN), *Random Forest* (RF) *dan Decision Tree (*DT) yang berbeda.

4. Hasil dan Pembahasan

Sebelum menyelami metode yang diusulkan, kami akan memperkenalkan pendekatan yang diusulkan secara singkat. Kami membagi alur kerja solusi yang diusulkan menjadi lima langkah. Langkah pertama adalah analisis data eksploratori, yang mengacu pada proses kritis dalam melakukan investigasi awal pada data untuk menemukan pola, menemukan anomali, menguji hipotesis (statistik inferensial), dan memeriksa asumsi dengan bantuan statistik deskriptif dan representasi grafis, lalu menerapkan teknik praproses yang sesuai pada langkah kedua. Pada langkah ketiga, menghitung bobot berdasarkan distribusi kelas (serangan). Setelah estimasi bobot, kami mengklasifikasikan sub-bagian menggunakan berbagai pengklasifikasi LGBM, *k-nearest neighbor* (KNN), *random forest* (RF), dan *algoritma decision tree* (DT).

4.1. Analisis Data Eksploratori

Analisis Data Eksploratori mengacu pada proses kritis melakukan investigasi awal pada data untuk menemukan pola, menemukan anomali, menguji hipotesis (statistik inferensial), dan memeriksa asumsi dengan bantuan statistik deskriptif dan representasi grafis

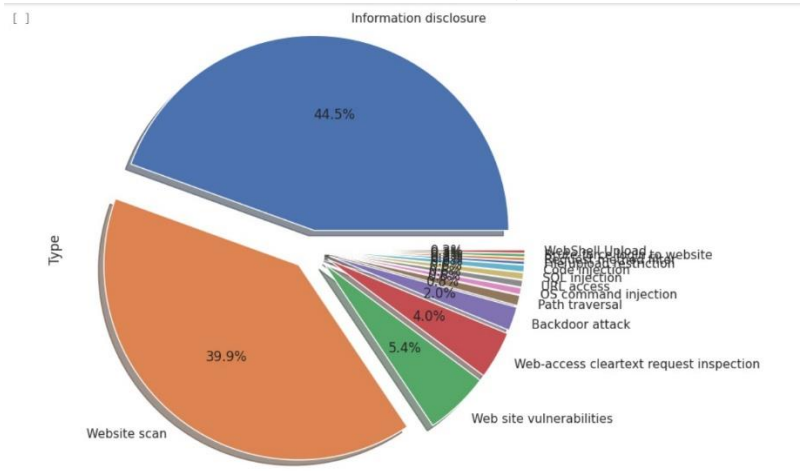
```
[ ]  # Read dataset - Logs WAF
     import io
     df = pd.read_csv(io.StringIO(Manefilenya['logswaff.csv'].decode('utf-8')))
```

```
[ ]  df.head
```

```
<bound method NDFrame.head of                       Type          Src IP Src Location Threat Level
0      Information disclosure   103.105.35.122    Indonesia       Medium
1      Information disclosure     182.2.41.232    Indonesia       Medium
2      Information disclosure      114.10.6.73    Indonesia       Medium
3    Web site vulnerabilities  110.164.147.131     Thailand         High
4      Information disclosure  180.242.214.227    Indonesia       Medium
..                        ...              ...          ...          ...
995              Website scan     47.128.48.14       Canada       Medium
996    Information disclosure   139.59.255.203    Singapore         High
997      OS command injection  110.164.147.131     Thailand         High
998           Path traversal   139.59.255.203    Singapore       Medium
999  Web site vulnerabilities   139.59.255.203    Singapore         High

[1000 rows x 4 columns]>
```

```
[ ]  # select with no duplicated data
     df = df[~df.duplicated()]
```

Gambar 1. Analisis Data Eksploratori



Gambar 2. Target serangan web

4.2. Mendeskripsikan Data

Salah satu langkah penting dalam penelitian adalah mendeskripsikan data. Hal ini dilakukan untuk membuat data yang telah dikumpulkan lebih mudah dipahami oleh pembaca.

Tabel 1. Mendeskripsikan data

	Type	Src IP	Src Location	Threat Level
count	353	353	353	353
unique	14	325	24	2
top	Information disclosure	110.164.147.131	Indonesia	Medium
freq	157	13	114	313

4.3. Label Encoder

Dalam pustaka Python yang disertakan dalam "SciKit Learn," label encoder berfungsi untuk mengubah data kategoris dan string menjadi angka numerik yang dapat dengan mudah dipahami oleh model.

```
# Import label encoder
from sklearn import preprocessing

# label_encoder object knows
# how to understand word labels.
label_encoder = preprocessing.LabelEncoder()

# Encode labels in column 'species'.
df['Type']= label_encoder.fit_transform(df['Type'])
df['Src Location']= label_encoder.fit_transform(df['Src Location'])
df['Threat Level']= label_encoder.fit_transform(df['Threat Level'])

df['Type'].unique()
df['Src Location'].unique()
df['Threat Level'].unique()
```

```
array([1, 0])
```

Gambar 3. Pelabelan

4.4. Praproses Data

Metode untuk menyiapkan data untuk penggunaan ekstraksi pengetahuan tingkat lanjut, atau, dengan kata lain, fase yang dimaksudkan untuk mengatasi masalah yang dapat mengganggu proses pemrosesan data.

[ ]

	Type	Src IP	Src Location	Threat Level
0	4	103.105.35.122	11	1
1	4	182.2.41.232	11	1
2	4	114.10.6.73	11	1
3	10	110.164.147.131	20	0
4	4	180.242.214.227	11	1

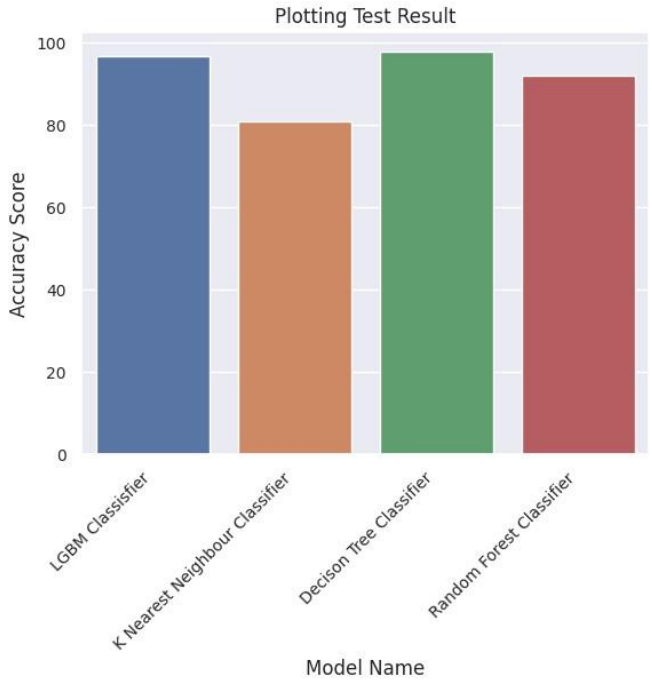
```
from sklearn.preprocessing import LabelEncoder

# Label Encoding
encoder = LabelEncoder() # method initialization

# Looping for columns except Survived
for c in dataset.columns[1:]:
    if(dataset[c].dtype=='object'): # if column type = object (like "Tiket" and "Sex")
        dataset[c] = encoder.fit_transform(dataset[c])
    else: # else get the self column value without encode
        dataset[c] = dataset[c]

dataset.head()
```

	Type	Src IP	Src Location	Threat Level
0	4	2	11	1
1	4	142	11	1
2	4	65	11	1
3	10	27	20	0
4	4	126	11	1

Gambar 4. Pemrosesan data

4.5. Klasifikasi

Hasil pengujian plotting diperoleh berdasarkan skor akurasi yang telah dilakukan, dan klasifikasi LGBM serta keputusan memiliki nilai yang cukup tinggi.



Gambar 5. Ploting test

5. Kesimpulan

Evaluasi model terbaik dari hasil yang diperoleh menunjukkan nilai akurasi sebesar 96,63% yang berarti hasilnya cukup baik. Hal ini menunjukkan bahwa nilai *recall* berarti 33 c/o data prediksi dibandingkan dengan total data aktual, sedangkan akurasi berarti terdapat 40 c/o data yang dapat diprediksi, dan skor F1 menyatakan terdapat sekitar 36,3 c/o perbandingan antara presisi dan *recall* yang tertimbang.

DAFTAR PUSTAKA

[1] Arunkumar, M., Kumar, K.A. GOSVM: Gannet optimization based support vector machine for malicious attack detection in cloud environment. Int. j. inf. tecnol. 15, 1653–1660 (2023). https://doi.org/10.1007/s41870-023-01192-z

[2] Sachdeva, S., Ali, A. Machine learning with digital forensics for attack classification in cloud network environment. Int J Syst Assur Eng Manag 13 (Suppl 1), 156–165 (2022). https://doi.org/10.1007/s13198-021-01323-4

[3] Naeem,M.R,Amin.R, Alshamrani.Sultan S.,Alshehri.A. Digital Forensics for Malware Classification: An Approach for Binary Code to Pixel Vector Transition. Computational Intelligence and Neuroscience.(2022). https://doi.org/10.1155/2022/6294058

[4] Kim, H., Kim, J., Kim, Y. et al. Design of network threat detection and classification based on machine learning on cloud computing. Cluster Comput 22 (Suppl 1), 2341–2350 (2019). https://doi.org/10.1007/s10586-018-1841-8

[5] Bijalwan.A. Botnet Forensic Analysis Using Machine Learning. Security and Communication Networks .(2020).https://doi.org/10.1155/2020/9302318

[6] Chakir et al., 2023 O. Chakir, A. Rehaimi, Y. Sadqi, M. Krichen, G.S. Gaba, A. Gurtov, et al. An empirical assessment of ensemble methods and traditional machine learning techniques for web-based attack detection in industry 5.0 J. King Saud Univ.-Comput. Informat. Sci., 35 (3) (2023), pp. 103-119

[7] Saran.N and Kesswani.N,A comparative study of supervised Machine Learning classifiers for Intrusion Detection in Internet of Things.Procedia Computer Science.Volume 218.(2023).Pages 2049-2057.https://doi.org/10.1016/j.procs.2023.01.181.

[8] Ahamed BS (2021) Prediction of Type-2 Diabetes using the *LGBM Classifier* methods and techniques. Turk J Comput Math Educ (TURCOMAT) 12(12):223–231

[9] Kunhare, Nilesh & Tiwari, Ritu & Dhar, Joydip. (2020). Particle swarm optimization and feature selection for intrusion detection system.S¯adhan¯a. 45. 10.1007/s12046-020-1308-5.

[10] Safavian, S. R., & Landgrebe, D. (1991). A survey of decision tree classifier methodology. IEEE transactions on systems, man, and cybernetics,21(3), 660-674.

[11] Priyanka,&Kumar,D.(2020).Decisiontreeclassifier:Adetailedsurvey.International Journal of Information and Decision Sciences,12(3),246-269.

[12] Liaw, Andy & Wiener, Matthew. (2001). Classification and Regression by RandomForest.Forest. 23.