Jurnal Inovasi Teknik dan Edukasi Teknologi, 3(1), 2023, 47-53
ISSN: 2797-7196 (online)
DOI:10.17977/um068v3i12023p47-53

# Klasifikasi Serangan Pada Jaringan Internet of Thing (IoT): Tinjauan Literatur Komparatif

**Rijal Akhdan Khairulah*, Roni Herdianto, Mohamad Arief Setiawan**
Universitas Airlangga, Indonesia, Jl. Dr. Ir. H. Soekarno, Kota SBY, Jawa Timur 60115, Indonesia
Universitas Negeri Malang, Jl. Semarang No. 5 Malang, Jawa Timur, Indonesia
Politeknik Negeri Malang, Jl. Soekarno Hatta No.9, Kota Malang, Jawa Timur 65141 Indonesia
*Penulis korespondensi, Surel: rijal.akhdan.khairullah-2020@ftmm.unair.ac.id

Paper received: 03-01-2023; revised: 15-01-2023; accepted: 30-01-2023

**Abstract**

The Internet of Things (IoT) is now an important part of human daily life, especially in the fields of industry, transportation, and health. However, the complexity and security vulnerabilities of IoT networks have led to an increase in cyberattacks that threaten user privacy and security. Early detection of attacks that will be carried out on IoT networks can prevent crimes that threaten user privacy and security. In this study, a comparative literature review was conducted on several Machine Learning (ML) and Deep Learning (DL) methods used to classify IoT network attacks. The results of the literature review show that the Random Forest (RF) method has very good performance in classifying attacks on IoT networks.

**Keywords:** attack classification; machine learning; deep learning; internet of things; cybersecurity

**Abstrak**

Internet of Things (IoT) sekarang menjadi bagian penting kehidupan sehari-hari manusia, terutama dalam bidang industri, transportasi, dan kesehatan. Namun, kompleksitas dan rentannya keamanan pada jaringan IoT menyebabkan peningkatan serangan siber yang mengancam privasi dan keamanan pengguna. Deteksi dini serangan yang akan dilakukan pada jaringan IoT dapat menghindarkan kejahatan yang mengancam privasi dan keamanan pengguna. Pada penelitian ini, dilakukan tinjauan literatur komparatif terhadap beberapa metode Machine Learning (ML) dan Deep Learning (DL) yang digunakan untuk mengklasifikasikan serangan jaringan IoT. Hasil tinjauan literatur menunjukkan bahwa metode Random Forest (RF) memiliki performa yang sangat baik dalam mengklasifikasikan serangan pada jaringan IoT.

**Kata kunci**: klasifikasi serangan; pembelajaran mesin; pembelajaran mendalam; Internet untuk segala; keamanan cyber

## 1. Pendahuluan

Internet of Things (IoT) merupakan sebuah alat yang mampu berkomunikasi dan mengirimkan data melalui jaringan tanpa interaksi dari manusia (Bimantara & Stiawan, 2021; Churcher et al., 2021; Kurniabudi et al., 2022).Konsep IoT ini diartikan sebagai sebuah kemampuan untuk menghubungkan objek yang cerdas dan memungkinkannya untuk berinteraksi dengan objek lain, lingkungan, maupun dengan peralatan komputasi cerdas lainnya melalui jaringan internet.Dalam perkembangannya Internet of Things belakangan ini sangatlah pesat, hal tersebut terlihat dari meningkatnya jumlah pengguna berbagai perangkat IoT dari waktu ke waktu (Rafsanjani et al., 2022). Perkembangan perangkat IoT menyebabkan perubahan di setiap aspek kehidupan manusia , diantaranya smart city, smart home, smart street, dan smart industry yang memanfaatkan internet untuk memantau informasi yang dibutuhkan. Namun, jaringan IoT yang kompleks itu sendiri menghadirkan tantangan untuk menjaga keamanan jaringan.

Kompleksitas jaringan IoT yang meliputi data, protokol, ukuran, komunikasi, standar, dan lainnya, menjaga keamanan dalam jaringan menjadi tantangan yang cukup besar. Jaringan yang kompleks dalam IoT juga dapat menjadi target mudah untuk disusupi penyerang dengan menggunakan malware, dan serangan cyberattack terus meningkat setiap tahunnya. Menurut Sandriana & Maulana (2022) sepanjang tahun 2021 terdapat lebih dari 1,6 miliar atau tepatnya 1.637.973.022 anomali lalulintas jaringan atau serangan siber yang terjadi diseluruh wilayah Indonesia (Riskilah et al., 2022). Salah satu ancaman serius yang ada pada jaringan IoT yaitu Distributed Denial of Service (DDOS) Serangan DDOS dapat menyebabkan suatu server menjadi sibuk dengan banyaknya permintaanpermintaan sehingga pengguna yang sah atau normal tidak dapat mengakses jaringan tersebut (Alfian & Stiawan, 2022; Nascita et al., 2022; Nihri et al., 2018). Serangan DoS dapat dilakukan dengan mengirim UDP atau ICMP dengan paket-paket besar dan jumlah yang banyak (Andika & Stiawan, 2018). Selanjutnya adalah dengan menggunakan kelemahan protokol seperti SYN flood. Serangan ini menyerang dengan memberi banyak permintaan yang membuat korban tidak dapat memproses permintaan yang sebenarnya. Yang terakhir adalah dengan menggunakan kelemahan dalam lapisan aplikasi seperti slowloris.

Dalam mengantisipasi serangan DoS di middleware IoT bisa dengan menggunakan *Intrusion Detection System* (IDS). Akan tetapi, tentunya IDS membutuhkan tingkat performansi dan akurasi yang tinggi dalam mendeteksi atau mengklasifikasi serangan DoS di middleware IoT sedangkan dengan kompleksitas jaringan IoT yang meliputi data, protokol, ukuran, komunikasi, standar, dan lainnya, menjaga keamanan dalam jaringan menjadi tantangan yang cukup besar. Oleh karena itu, penggunaan metode *Machine Learning* (ML) dan *deep learning* diperlukan untuk meningkatkan kinerja IDS dalam mendeteksi serangan pada jaringan kompleks IoT. Pada tinjauan literatur ini akan membahas apa saja metode yang digunakan dalam memprediksi atau mendeteksi serangan pada IoT dan menijau perbedaan antar sumber literatur.

## 2. Metode

Studi literatur adalah jenis metode pendekatan yang dilakukan pada penulisan artikel ini. Sebelum dilakukan langkah-langkah studi literatur, ditetapkan dahulu pertanyaan penelitian (Research Questions (RQ)). Pertanyaan penelitian dari studi literatur ini adalah: (1) RQ1 = Apa saja jenis serangan pada jaringan IoT; (2) RQ2 = Apa saja model ML yang dapat digunakan dalam mengklasifikasikan serangan pada jaringan IoT?; (3) Kinerja metode apa menunjukkan performa yang paling baik?. Secara sistematis langkah-langkah melakukan studi literatur dijelaskan sebagai berikut.

### 2.1. Menentukan kata kunci pencarian sesuai topik

Kata kunci yang ditentukan dalam penelitian ini adalah “Klasifikasi; serangan IoT; Machine Learning”. Pembatasan tahun terbit artikel dilakukan dalam menambang artikel untuk memastikan novelty dan tren riset. Artikel dibatasi terbit antara tahun 2018-2022. Google scholar dijadikan dasar tempat pencarian platform database artikel jurnal karena alasan sebagai berikut: (1) google scholar menyediakan akses ke artikel, paper, dan publikasi ilmiah dari berbagai disiplin ilmu, (2) google scholar mudah digunakan dan dapat diakses oleh siapa saja dengan koneksi internet, (3) google scholar adalah sumber informasi ilmiah yang gratis.

### 2.2. Hasil pencarian awal dan filtering data

Hasil pencarian awal dari Google scholar didapatkan sebanyak 1.120 artikel sesuai penyaringan data untuk mempersempit pencarian berdasarkan kriteria tertentu, seperti tanggal publikasi, penulis, atau jenis publikasi ilmiah. Kemudian data diolah dengan aplikasi pengolah data agar dapat dianalisis lebih lanjut. Setelah dilakukan filtering 1.120 artikel maka didapatkan 20 artikel yang relevan dengan topik yang diteliti.

### 2.3. Analisis data

Analisis data dilakukan berupa pemeriksaan abstrak artikel yang diperoleh dalam hasil pencarian. Jika abstraknya relevan dengan topik penelitian, maka artikel akan disimpan. Kemudian artikel-artikel yang disimpan dibaca dengan cermat dan dihubungkan dengan topik penelitian. Setelahnya adalah mencatat poin-poin penting yang ditemukan dan bagaimana artikel tersebut dapat berkontribusi pada penulisan studi literatur ini. Terakhir jika masih terdapat kekurangan data artikel, maka akan dilakukan pencarian artikel tambahan menggunakan kata kunci tambahan atau dengan melihat daftar referensi di dalam artikel-artikel yang telah ditemukan. Hal tersebut dilakukan untuk mengembangkan argumen penelitian agar lebih kuat.

### 2.4. Menjawab pertanyaan penelitian dan membuat simpulan

Tahap terakhir adalah menjawab tiga pertanyaan penelitian yang sudah ditentukan sebelumnya dan membuat simpulan sebagai penutup dari studi literatur yang dilakukan.

## 3. Hasil dan Pembahasan

Tujuan dari literatur review ini adalah untuk meninjau dan membandingkan berbagai metode ML dan deep learning dalam mengklasifikasikan serangan pada jaringan IoT. Dalam melakukan literatur review ini, peneliti mengumpulkan dan menganalisis berbagai sumber literatur terbaru yang terkait dengan topik ini (Tabel 1). Pada sumber literatur yang telah dikumpulkan tersebut menunjukkan bahwa ada beberapa jenis serangan yang umum terjadi pada jaringan IoT, seperti serangan *denial-of-service* (DoS), serangan *man-in-the-middle* (MitM), serangan *phishing*, dan serangan *malware*. Selain itu peneliti juga menemukan bahwa terdapat berbagai jenis algoritma ML dan *deep learning* yang telah digunakan untuk klasifikasi serangan pada jaringan IoT, seperti algoritma *Decision Tree* (DT), *naïve bayes* (NB), *Logistic Regression* (LR), *Support Vector Machine* (SVM), *Random Forest* (RF), dll. Ada beberapa tahapan penelitian yang harus dilakukan untuk dapat mendeteksi serangan yang terjadi pada jaringan kompleks IoT. Tahapan pertama yaitu, pengumpulan data, lalu Preprocessing & ekstraksi fitur, kemudian klasifikasi.

**Tabel 1. Hasil Pencarian dan Filtering Data Artikel**

| Tahun Terbit | Referensi | Jumlah |
|---|---|---|
| 2018 | (Andika & Stiawan, 2018; Nihri et al., 2018) | 2 |
| 2019 | (Alsamiri & Alsubhi, 2019; Hasan et al., 2019) | 2 |
| 2020 | (Karanja et al., 2020; Naeem et al., 2020; Sofa & Subiyanto, 2020). | 3 |
| 2021 | (Afifaturahman, 2021; Aprianti & Deris, 2021; Bimantara & Stiawan, 2021; Churcher et al., 2021) | 4 |
| 2022 | (Alfian & Stiawan, 2022; Azmi, 2022; Kurniabudi et al., 2022; Marlo & Stiawan, 2022).<br>(Nascita et al., 2022; Rafsanjani et al., 2022; Riskilah et al., 2022), | 9 |

| | | |
|---|---|---|
| | (Sandriana & Maulana, 2022; Winanto et al., 2022) | |
| Total | | 20 |

### 3.1. RQ 1 (Apa saja jenis serangan pada jaringan IoT?)

Pengumpulan data dari masing masing sumber literatur berbeda beda begitu juga dengan jenis serangan yang dideteksi tiap literatur juga berbeda. Berikut merupakan dataset dan jenis serangan yang dianalisis pada penelitian dari beberapa sumber literur yang disajikan pada Tabel 2.

**Tabel 2. Jenis Serangan pada Jaringan IoT (RQ1)**

| No | Referensi | Jenis Serangan | Deskripsi Pengambilan |
|---|---|---|---|
| 1 | (Alsamiri & Alsubhi, 2019) | Probing, DoS, dan Information Theft | Dataset yang digunakan adalah Bot-IoT dataset yang dibuat di Cyber Range Lab di Australian Centre for Cyber Security (ACCS) |
| 2 | (Churcher et al., 2021) | Data exfiltration, DoS HTTP, DoS TCP, DoS UDP, DDoS HTTP, DDoS TCP, DDoS, UDP, Keylogging, OS Scan dan Service Scan | Dataset yang digunakan adalah Bot-IoT yang di-submit ke situs IEEE pada 16 Oktober 2019 dan dibuat oleh University of New South Wales (UNSW) |
| 3 | (Hasan et al., 2019) | DoS, Probing, Malicious Control, Malicious Operation, Scan, Spying, dan Wrong Setup | Dataset berasal dari open sorce kaggele dataset diciptakan dari lingkungan IoT virtual menggunakan Distributed Smart Space Orchestration System (DS2OS) untuk menghasilkan data sintetik. |
| 4 | (Kurniabudi et al., 2022) | Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet dan DDoS | Dataset berasal dari dataset CICIDS2017yang berisi serangan umum yang jinak dan menyerupai data dunia nyata (PCAP) sebenarnya |
| 5 | (Nascita et al., 2022; Sandriana & Maulana, 2022) | DDoS, Botnet, dan Scan | Dataset yang digunakan bernama IOT-23 dataset yang dikumpulkan di Laboratorium Stratosphere Universitas Teknik Ceko antara 2018 dan 2019. |
| 6 | (Riskilah et al., 2022) | dictionary attack dan DDoS | Dataset menggunakan data yang diambil sendiri dan<br>data yang sudah ada sebelumnya |
| 7 | (Winanto et al., 2022) | TCP flood dan zbassocflood | Dataset yang digunakan berasal dari dataset IoT yang kompleks dari Comnets Lab Unsri |

Pada tahapan preprocessing adalah langkah membuat data lebih konsisten dan menghilangkan atribut yang kurang dominan untuk mereduksi data namun tetap mendapatkan data yang akurat (Sandriana & Maulana, 2022). Dengan kata lain preprocessing ini mengubah data supaya data siap dipakai. Preprocessing yang dilakukan meliputi menghilangkan data ganda, mengatasi masalah *Missing Value,* transformasi data data menjadi struktur yang sesuai untuk pembelajaran mesin. (Alsamiri & Alsubhi, 2019; Kurniabudi et al., 2022; Nihri et al., 2018).

Setelah menyiapkan data selanjutnya melakukan ekstraksi/seleksi fitur. Pemilihan fitur ini digunakan untuk mengetahui *feature* yang berpengaruh terhadap label (Riskilah et al., 2022). Dengan begitu fitur yang memiliki informasi yang relevan akan membantu model mengklasifikasikan data dengan lebih baik sedangkan fitur yang tidak mengandung informasi tidak akan digunakan karena dapat menyebabkan tingkat akurasi model buruk.Ekstraksi fitur yang bisa digunnakan seperti, seleksi fitur *ExtraTreeClassifier*, *Principal Component Analysis* (PCA), *teknik univariate feature selection*, dll.

### 3.2. RQ 2 (Apa saja model ML yang dapat digunakan dalam mengklasifikasikan serangan pada jaringan IoT?)

*Machine Learning* dapat digunakan untuk mengekstrak informasi dari kumpulan data. Dengan menggunakan perhitungan statistik dan algoritma matematis, ML dapat mengungkap informasi, pola, dan hubungan tersembunyi antar atribut dalam kumpulan data (Nihri et al., 2018). Hal ini sangat berguna untuk mendeteksi data yang mencurigakan. Pada tahapan klasifikasi ini yang dilakukan yaitu melakukan training data dan pengujian testing data pada algoritma ML yang akan dianalisis. Terdapat beberapa model ML yang dapat digunakan dalam mengklasifikasikan serangan pada jaringan IoT, dapat dilihat pada Tabel 3 terdapat metode algoritma klasifikasi yang digunakan dari beberapa sumber literatur.

**Tabel 3. Metode algoritma klasifikasi (RQ2)**

| No | Algoritma Machine Learning /Deep Learning | Literatur | Total |
|---|---|---|---|
| 1 | K-Nearest Neighbor (KNN) | (Afifaturahman, 2021; Alsamiri & Alsubhi, 2019; Churcher et al., 2021; Karanja et al., 2020; Riskilah et al., 2022; Sandriana & Maulana, 2022). | 6 |
| 2 | Naive Bayes (NB) | (Afifaturahman, 2021; Alsamiri & Alsubhi, 2019; Aprianti & Deris, 2021; Churcher et al., 2021; Karanja et al., 2020; Marlo & Stiawan, 2022; Nascita et al., 2022; Riskilah et al., 2022; Sofa & Subiyanto, 2020). | 9 |
| 3 | Support Vector Machine (SVM) | (Alfian & Stiawan, 2022; Azmi, 2022; Churcher et al., 2021; Hasan et al., 2019). | 4 |
| 4 | Random Forest (RF) | (Alsamiri & Alsubhi, 2019; Churcher et al., 2021; Hasan et al., 2019; Karanja et al., 2020; Kurniabudi et al., 2022; Nascita et al., 2022). | 8 |
| 5 | AdaBoost | (Alsamiri & Alsubhi, 2019) | 1 |
| 6 | Iterative Dichotomiser 3 (ID3) | (Alsamiri & Alsubhi, 2019) | 1 |
| 7 | C4.5 | (Andika & Stiawan, 2018) | 1 |

Pada Table 3 tersebut menunjukkan bahwa algoritma ML yang paling banyak digunakan dalam penelitian klasifikasi serangan pada jaringan IoT yaitu algoritma *Naïve Bayes* (NB),

*Random Forest* (RF), dan kemudian *K-Nearest Neighbor* (KNN). Namun algoritma *Support Vector Machine* (SVM), *Artificial Neural Network* (ANN), dan juga *Decision Tree* (DT) juga cukup banyak digunakan. Pada tinjauan literatur ini akan meninjau perbedaan hasil analisis model ML yang banyak digunakan pada sumber literatur.

Penggunaan Algoritma KNN, NB, dan RF lebih sering digunakan dalam penelitian deteksi serangan pada jaringan IoT. Pada penelitian (Alsamiri & Alsubhi, 2019; Churcher et al., 2021; Karanja et al., 2020) 3 algoritma tersebut digunakan dalam mengklasifikasikan serangan pada jaringan IoT.Pada penelitian (Alsamiri & Alsubhi, 2019), Alsamiri & Alsubhi melakukan beberapa fase dalam menguji model machine lerningnya, fase pertama peneliti menerapkan algoritma ML pada setiap serangan secara terpisah lalu pada fase selanjutnya peneliti menerapkan algoritma ML pada seluruh dataset menggunakan 13 fitur, kemudian fase terakhir peneliti menerapkan algoritma ML pada seluruh dataset dengan tujuh fitur terbaik yang diperoleh dari seleksi fitur.didapatkan bahwa pada fase pertama algoritma KNN memiliki performa terbaik sedangkan algoritma NB memiliki skor terendah akan tetapi dibandingkan dengan algoritma KNN, NB lebih cepat dalam prosesnya.Lalu pada fase kedua tidak terdapat banyak perbedaan jika melihat skor yang didapat pada fase pertama. Pada fase ketiga sangat terlihat adanya perbedaan yaitu terdapat peningkatan kebaikan model dari semua algoritma ML yang diuji dilihat dari skor yang didapat.Walaupun tetap KNN memiliki performa terbaik sedangkan algoritma NB memiliki skor terendah jika dilihat dari skor yang didapat.Tetapi jika melihat dibandingkan dengan waktu pemrosesan algoritma NB lebih unggul daripada KNN. Untuk algoritma RF lebih stabil dimana perbedaan akurasi yang didapat jika dibandingkan dengan algoritma KNN tidak terpaut jauh, untuk waktu pemrosesan juga tidak membutuhkan waktu yang lama seperti algoritma KNN.

Pada penelitian Churcher et al. (2021) melakukan dua pengujian klasifikasi yaitu klasifikasi biner dan multi-kelas pada dataset Bot-IoT. Pengujian klasifikasi biner ini merupakan pengujian algoritma ML pada setiap serangan secara terpisah sedangkan multi-kelas ini pengujian algoritma ML pada semua baris dari semua kumpulan dataset serangan .Hasil yang didapatkan dari penelitian tersebut yaitu algoritma RF lebih unggul dalam klasifikasi biner.Namun, dalam klasifikasi multi-kelas, KNN lebih unggul dengan keunggulan 4% lebih tinggi daripada algoritma RF. Sedangkan untuk algoritma NB ini pada pengujian klasifikasi biner hasil yang didapat tidak jauh berbeda dengan algoritma KNN lalu untuk pengujian klasifikasi multi-kelas pun tidak jauh berbeda dengan algoritma RF dengan perbedaan 1% lebih rendah dari algoritma RF.

Berbeda dengan dua penelitian sebelumnya pada penelitian (Karanja et al., 2020), Karanja, dkk melakukan klasifikasi serangan pada jaringan IoT menggunakan jenis data gambar yaitu dengan *Image Texture Features*.dalam pengujiannya RF, NB, dan KNN digunakan sebagai pengklasifikasi data gambar malware. Hasil dari klasifikasi yang dilakukan menunjukkan bahwa RF memiliki performa yang lebih baik disemua kelas dibandingkan dengan dua algoritma ML lainnya. Akan tetapi bukan berarti hanya algoritma RF yang baik dalam mengklasifikasi data gambar malware melainkan dari hasil yang didapat menunjukkan bahwa semua metode memilik nilai di atas rata-rata dilihat dari nilai akurasi keseluruhan yaitu, RF memiliki nilai akurasi 97%, KNN sebesar 80%, dan NB sebesar 92%.

Selain tiga algoritma tadi terdapat beberapa algoritma yang juga cukup banyak digunakan dalam mengklasifikasikan serangan pada jaringan IoT, yaitu algoritma SVM, ANN, dan juga DT.

Pada penelitian (Hasan et al., 2019), Hasan, dkk menggunakan algoritma SVM, DT, ANN, LR dan RF dalam mendeteksi serangan dan anomali pada sensor IoT. *Five-fold cross-validation* dilakukan pada dataset menggunakan masing masing metode ML tersebut. Hasil dari analisis yang dilakukan menunjukkan bahwa algoritma RF dan ANN memiliki kinerja yang baik dalam pelatihan maupun pengujian. Pada tahap testing, DT memiliki performa yang buruk akan tetapi seiring sampel bertambah performa nya membaik dan mendekati performa dari algoritma RF dan ANN. Sedangkan performa SVM dan LR bekerja lebih lemah daripada teknik lain dalam tahap *Training*. Begitu juga dengan tahap *Testing*, SVM dan LR awalnya memiliki performa yang lebih baik dari teknik lainnya, tetapi pada tiga *fold* terakhir performa nya tidak membaik dan akhirnya kinerjanya lebih buruk dari tiga metode lainnya. Walaupun begitu pada penelitian ini LR dan SVM dapat dikatakan bekerja dengan baik pada dataset yang digunakan peneliti (Hasan et al., 2019) tetapi tidak sebagus pengklasifikasi lainnya.

### 3.3. RQ 3 (Kinerja algoritma apa menunjukkan performa yang paling baik?)

Selain penelitian itu, pada penelitian yang dilakukan (Nascita et al., 2022) ini menggunakan algoritma ML NB,DT,BG, dan RF dalam mengklasifikasikan serangan pada jaringan IoT.Tidak hanya menggunakan ML tetapi Nascita, dkk juga menggunakan teknik *Deep Learning* (DL) pada penelitiannya. Hasil dari analisis yang dilakukan menunjukkan bahwa algoritma RF memiliki performa sedikit lebih baik dari algoritma BG dilihat dari nilai accuracy dan F-measure yang didapat.Selain itu, performa yang diperoleh semua algoritma ML memiliki kenerja yang bagus kecuali algoritma NB, yang menunjukkan nilai akurasi 37,60% dan ukuran-F 25,44%. Sedangkan, arsitektur DL menunjukkan hasil yang lebih buruk dari metode ML.

## 4. Simpulan

Rentannya keamanan pada jaringan komplek IoT memicu banyaknya penelitian yang dilakukan untuk mengatasi masalah ini. Penelitian-penelitian tersebut bertujuan untuk meningkatkan keamanan dan privasi pada perangkat-perangkat IoT serta menemukan solusi untuk mengatasi ancaman keamanan yang mungkin terjadi. Penelitian yang dilakukan salah satunya mengembangkan alat deteksi serangan pada jaringan IoT. Pada tinjauan literatur ini peneliti mengumpulkan sumber literatur yang membahas mengenai penggunaan ML dalam membantu dalam mengklasifikasi/mendeteksi serangan pada jaringan IoT. Dari sumber literatur yang didapat peneliti menemukan bahwa terdapat berbagai jenis algoritma ML dan deep learning yang telah digunakan untuk klasifikasi serangan pada jaringan IoT. Dari metode ML yang ditemukan pada sumber literatur, metode yang paling banyak digunakan yaitu metode NB, RF, dan kemudian KNN. Namun algoritma SVM, ANN, dan juga DT juga cukup banyak digunakan. Dari banyak nya metode klasifikasi yang digunakan pada sumber literatur. Kinerja metode RF menunjukkan performa yang sangat baik. Hal ini didukung oleh hasil metode RF dari tiap pengujian dan evaluasi yang tinggi dalam memprediksi dan mengklasifikasikan data serangan dari berbagai sumber data literatur yang berbeda beda. Oleh karena itu, metode RF ini dapat dijadikan sebagai alternatif yang potensial dalam membantu meningkatkan kinerja IDS dalam mendeteksi serangan pada jaringan kompleks IoT.

## Daftar Rujukan

Afifaturahman, A. D. (2021). Perbandingan algoritma k-nearest neighbour (knn) dan naive bayes menggunakan parameter metric accuracy, sensitivity dan specificity pada Intrusion Detection System (IDS) (Doctoral Dissertation). Universitas Siliwangi.

Alfian, B., & Stiawan, D. (2022). Klasifikasi serangan udp flood pada jaringan internet of things (iot) menggunakan metode Support Vector Machine (SVM). Sriwijaya University.

Alsamiri, J., & Alsubhi, K. (2019). Internet of things cyber attacks detection using machine learning. International Journal of Advanced Computer Science and Applications, 10(12).

Andika, R., & Stiawan, D. (2018). Pengenalan pola serangan denial of service (udp flood) pada jaringan Internet of Things (IOT) dengan algoritma decision tree C4. 5 (Doctoral dissertation, Sriwijaya University). Sriwijaya University.

Aprianti, W., & Deris, S. (2021). Implementasi Principal Component Analysis (PCA) Dan Algoritma Naïve Bayes Classifier Pada Klasifikasi Botnet di Jaringan Internet of Things (IoT). Sriwijaya University.

Azmi, M. M. (2022). Deteksi serangan ddos tingkat rendah pada SD-IOT menggunakan svm dan logistic regression coefficient (Doctoral dissertation, Universitas Muhammadiyah Malang). Universitas Muhammadiyah Malang.

Bimantara, A., & Stiawan, D. (2021). Klasifikasi botnet pada jaringan internet of things (iot) menggunakan autoencoder dan Artificial Neural Network (ANN) (Doctoral dissertation, Sriwijaya University). Sriwijaya University.

Churcher, A., Ullah, R., Ahmad, J., Ur Rehman, S., Masood, F., Gogate, M., & Buchanan, W. J. (2021). An experimental analysis of attack classification using machine learning in IoT networks. Sensors, 21(2), 446.

Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things, 7, 100059.

Karanja, E. M., Masupe, S., & Jeffrey, M. G. (2020). Analysis of internet of things malware using image texture features and machine learning techniques. Internet of Things, 9, 100153.

Kurniabudi, K., Harris, A., & Rosanda, E. (2022). Optimalisasi Seleksi Fitur Untuk Deteksi Serangan Pada IoT Menggunakan Classifier Subset Evaluator. JURIKOM (Jurnal Riset Komputer), 9(4), 885–893.

Marlo, C., & Stiawan, D. (2022). Visualisasi data serangan udp flood pada jaringan internet of things (iot) menggunakan algoritma naive bayes classifier (Doctoral dissertation, Sriwijaya University). Sriwijaya University.

Naeem, H., Ullah, F., Naeem, M. R., Khalid, S., Vasan, D., Jabbar, S., & Saeed, S. (2020). Malware detection in industrial internet of things based on hybrid image visualization and deep learning model. Ad Hoc Networks, 105, 102154.

Nascita, A., Cerasuolo, F., Di Monda, D., Garcia, J. T. A., Montieri, A., & Pescape, A. (2022). Machine and deep learning approaches for IoT attack classification. IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 1–6.

Nihri, H., Pramukantoro, E. S., & Trisnawan, P. H. (2018). Pengembangan IDS Berbasis J48 Untuk Mendeteksi Serangan DoS Pada Perangkat Middleware IoT. Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer E-ISSN, 2548, 964X.

Rafsanjani, M. S., Suryani, V., & Pahlevi, R. R. (2022). Deteksi Serangan Botnet Pada Jaringan Internet Of Things Menggunakan Algoritma Random Forest (rf). EProceedings of Engineering, 9(3).

Riskilah, M. K., Yulianto, F. A., & Jadied, E. M. (2022). Studi Analisis Algoritma NaÏve Bayes Untuk Sistem Deteksi Intrusi Pada Internet Of Things. EProceedings of Engineering, 9(3).

Sandriana, A., & Maulana, F. (2022). Klasifikasi serangan malware terhadap lalu lintas jaringan Internet of Things menggunakan Algoritma K-Nearest Neighbour (K-NN). E-JOINT (Electronica and Electrical Journal Of Innovation Technology), 3(1), 12–22.

Sofa, E. L., & Subiyanto, S. (2020). Routing Attacs pada Internet Of Things Berbasis Smart Intrution Detecion System. Jurnal Teknologi Informasi Dan Ilmu Komputer, 7(2), 329–338.

Winanto, E. A., Kurniabudi, K., Sharipuddin, S., Wijaya, I. S., & Sandra, D. (2022). Deteksi Serangan pada Jaringan Kompleks IoT menggunakan Recurrent Neural Network. JURIKOM (Jurnal Riset Komputer), 9(6), 1996–2002.