Jurnal Informatika dan Rekayasa Perangkat Lunak ISSN 2656-2855
Vol. 6, No. 2, September 2024, Hal. 472-479 e-ISSN 2685-5518

Deteksi Serangan Denial of Service (DoS) dan Spoofing pada Internet of Vehicles menggunakan Algoritma K-Nearest Neighbor (KNN)

Wildanil Ghozi[1], **Fauzi Adi Rafrastara**[2*], **Ramadhan Rakhmat Sani**[3], **Abdussalam**[4]
[1,2,4]Program Studi Teknik Informatika, Fakultas Ilmu Komputer
[3] Program Studi Sistem Informasi, Fakultas Ilmu Komputer
Universitas Dian Nuswantoro
[*]Email: fauziadi@dsn.dinus.ac.id

Abstrak

Implementasi teknologi Internet of Things pada kendaraan bermotor mengalami peningkatan dari waktu ke waktu dan dikenal dengan istilah Internet of Vehicle (IoV). IoV semakin dibutuhkan masyarakat karena dapat menghadirkan kenyamanan, keamanan, dan efisiensi dalam berkendara. Sayangnya, penggunaan teknologi internet pada IoV justru memunculkan potensi serangan siber, seperti Denial of Service (DoS) dan Spoofing. Intrusion Detection System pada IoV belum sepenuhnya berjalan dengan baik mengingat teknologi ini juga tergolong baru. Oleh karena itu, dengan adanya potensi ancaman sekaligus dampak yang dihasilkan menjadikan penelitian tentang hal ini menjadi urgent untuk dilakukan. Penelitian ini bertujuan untuk mengevaluasi performa algoritma klasifikasi k-Nearest Neighbor (kNN) dalam mendeteksi serangan siber pada IoV. Kelas yang diprediksi pada penelitian ini berjumlah enam, yaitu: Benign, DoS, Gas-Spoofing, Steering Wheel-Spoofing, Speed-Spoofing, dan RPM-Spoofing. Dua jenis serangan pada IoV tersebut (DoS dan Spoofing) beresiko menghadirkan gangguan operasional pada kendaraan yang dapat membahayakan pengemudi dan pengguna jalan lainnya. Dataset yang digunakan adalah dataset publik bernama CIC IoV2024. Performa algoritma kNN tersebut juga dibandingkan dengan tiga algoritma lain sebagai state-of-the-arts, seperti Naïve Bayes, Deep Neural Network, dan Random Forest. Hasilnya, k-Nearest Neighbor (kNN) mendapatkan performa terbaik dengan skor 98.7% untuk metrik akurasi maupun F1-Score. kNN mengungguli Naïve Bayes yang berada di urutan ke-dua, dengan skor 98.1% untuk akurasi dan 98.0% untuk F1-Score. Selanjutnya, algoritma kNN dapat direkomendasikan sebagai classifier dalam pengembangan intrusion detection system pada IoV.

***Kata kunci**: Internet of Vehicles, Deteksi Serangan, kNN, DoS, Spoofing*

Abstract

The implementation of Internet of Things (IoT) technology in motor vehicles has been increasing over time and is known as the Internet of Vehicles (IoV). IoV is becoming more essential to society as it provides comfort, safety, and efficiency in driving. Unfortunately, the use of internet technology in IoV brings the potential for cyber-attacks, such as Denial of Service (DoS) and Spoofing. Intrusion Detection Systems in IoV have not yet fully matured, as this technology is still relatively new. Therefore, the potential threats and their significant impact make research on this topic urgently needed. This study aims to evaluate the performance of the k-Nearest Neighbor (kNN) classification algorithm in detecting cyber-attacks on IoV. The predicted classes in this study consist of six categories: Benign, DoS, Gas-Spoofing, Steering Wheel-Spoofing, Speed-Spoofing, and RPM-Spoofing. These two types of attacks on IoV (DoS and Spoofing) pose risks to the operational safety of vehicles, which can endanger drivers and other road users. The dataset used is a public dataset called CIC IoV2024. The performance of the kNN algorithm is also compared to three other state-of-the-art algorithms, including Naïve Bayes, Deep Neural Network, and Random Forest. The results show that k-Nearest Neighbor (kNN) achieved the best performance with a score of 98.7% for both accuracy and F1-Score metrics. kNN outperformed Naïve Bayes, which ranked second with a score of 98.1% accuracy and 98.0% F1-Score. Thus, the kNN algorithm can be recommended as a classifier in the development of an intrusion detection system for IoV.

***Kata kunci**: Internet of Vehicles, Deteksi Serangan, kNN, DoS, Spoofing*

PENDAHULUAN

Dalam dunia modern, istilah internet of things (IoT) menjadi umum digunakan pada kehidupan sehari-hari (Chung and Cho, 2022). Teknologi IoT telah berkembang luas dan merambah hampir ke seluruh bidang kehidupan, mulai dari terkair urusan rumah tangga, perkantoran, industrial, hingga pada kendaraan. Penerapan teknologi IoT pada kendaraan disebut dengan internet of Vehicle (IoV) (Wei, 2024). Integrasi antara industri kendaraan, elektronika, dan industri-industri lainnya dengan IoT telah menghasilkan sitem transportasi yang bersih dan efisien (Wang and Wang, 2021).

Pada teknologi IoV, terjadi komunikasi atau pertukaran informasi antar perangkat-perangkat yang terhubung. Terdapat beberapa jenis komunikasi dalam teknologi IoV, diantaranya yaitu: (1) Vehicle to vehicle (V2V), merupakan komunikasi IoV dari satu kendaraan dengan kendaraan lainnya; (2) Vehicle to Infrastructure (V2I), merupakan komunikasi antara kendaraan dengan infrastruktur pendukungnya; (3) Vehicle to ecosystem (V2E), merupakan komunikasi IoV antara kendaraan dengan ekosistem pendukungnya; (4) Vehicle to Surroundings (V2S), merupakan komunikasi antara kendaraan dengan segala sesuatu di sekitarnya; dan (5) Vehicle to everythings (V2X), merupakan komunikasi IoV pada segala jenis komunikasi seperti V2V, V2G, hingga V2H. (Islam *et al.*, 2022; Korium *et al.*, 2024). Semua mode komunikasi pada IoV tersebut menghasilkan pertukaran informasi yang berguna untuk mendukung fasilitas *driver assistance, traffic management,* dan *safety improvements* pada kendaraan (Djenouri *et al.*, 2024).

Implementasi IoV dapat meningkatkan keamanan, kenyamanan, dan efisiensi dalam kendaraan (Qureshi *et al.*, 2021). Manfaat lain yang dapat dihasilkan dengan IoV adalah kemampuan memantau kondisi kendaraan hingga *smart parking* yang memungkinkan kendaraan untuk menemukan area parkir serta mengarahkan kendaraan ke area tersebut secara mandiri (Kaur and Garg, 2023). Sementara itu, contoh manfaat penerapan IoV dalam bisnis diantaranya adalah IoV dapat mendukung operasional perusahaan pengiriman dengan menemukan rute perjalanan paling optimal, melacak proses pengiriman secara real-time, serta memberikan informasi estimasi waktu pengiriman yang akurat kepada pelanggan (Djenouri *et al.*, 2024). Dengan berbagai kemampuan tersebut, maka tidak mengherankan jika IoV memiliki peran yang penting pada pengembangan teknologi *Intelligent Transportation System (ITS)* (Haodudin Nurkifli and Hwang, 2023; Chen *et al.*, 2024).

Komunikasi pada teknologi IoV melibatkan internet untuk mengirimkan data dari kendaraan menuju ke pusat kontrol. Penggunaan internet pada komunikasi IoV dapat memunculkan celah keamanan dan berisiko tinggi. Serangan-serangan pada sistem IoV terus mengalami peningkatan. Dua serangan yang sedang berkembang saat ini yaitu Denial of Service (DoS) dan serangan Spoofing (Neto *et al.*, 2024). Dua jenis serangan tersebut bukan hanya membahayakan sistem, namun juga dapat membahayakan pengguna, kendaraan, dan lingkungan sekitar (Rafrastara, Ghozi and Wardoyo, 2024). Untuk menjaga keamanan sistem IoV, dibutuhkan metode yang dapat mendeteksi serangan-serangan tersebut secara efektif sehingga sistem IoV dapat terhindar dari kegagalan sistem.

TINJAUAN PUSTAKA

Pada penelitian yang dilakukan oleh (Neto *et al.*, 2024), 4 algoritma diukur untuk menentukan algoritma yang paling efektif dalam mendeteksi serangan siber pada IoV. Ke-empat algoritma tersebut, yaitu: Logistic Regression, AdaBoost, Deep Neural Network, dan Random Forest. Pengujian dilakukan pada 2 jenis dataset, yaitu Binary dan Decimal. Hasilnya, pada Binary maupun Decimal dataset, Deep Neural Network mendapatkan performa terbaik. Skor yang diperoleh pada Binary Dataset, yaitu 95% untuk akurasi dan 63% untuk F1-Score. Sedangkan pada Decimal Dataset, skor yang diperoleh Deep Neural Network adalah 96% untuk akurasi dan 78% untuk F1-Score. Sayangnya, validasi yang digunakan pada penelitian ini adalah split validation, sehingga rentan terhadap overfitting.

Penelitian lain terkait deteksi serangan pada IoV juga dilakukan oleh (Ahmed, Jeon and Ahmad, 2023). Pada penelitian ini, dataset yang digunakan adalah CAN-intrusion-dataset. Dataset tersebut memuat tiga jenis serangan, seperti DoS Attack, Fuzzy Attack, dan Attack Free State. Metode yang diusulkan oleh peneliti adalah VGG-16, yaitu algoritma berbasis Deep

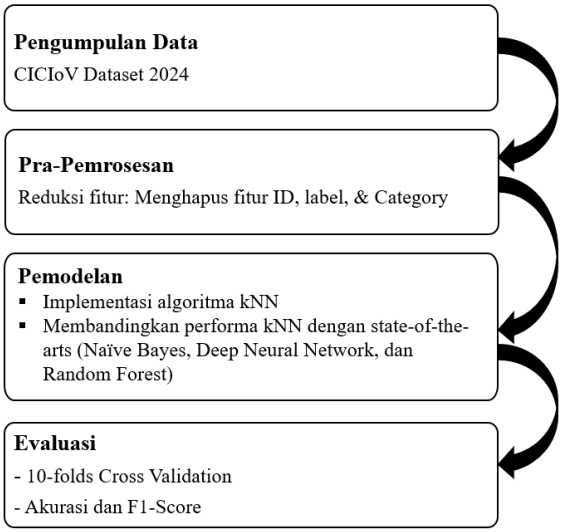
Learning. Sebagai hasil, VGG-16 berhasil mengungguli 5 algoritma lain, seperti kNN, Random Forest, Gradient Boosting, AdaBoost, dan SVM, dengan nilai akurasi sebesar 96%. Di sini, metode pemisahan data training dan testing yang digunakan adalah Split Validation, dengan rasio 70% untuk training dan 30% untuk testing. Tanpa menggunakan metode Cross-Validation, maka akan meningkatkan potensi terjadinya overfitting.

Peneliti pada (Rafrastara, Ghozi and Wardoyo, 2024) juga meneliti tentang deteksi serangan pada IoV. Algoritma yang diuji adalah Naive Bayes, Decision Tree, dan Logistic Regression. Performa tertinggi diperoleh algoritma Naive Bayes, dengan skor 98.1% baik untuk akurasi maupun F1-Score.

Mengingat tingkat fatalitas akibat kesalahan deteksi pada serangan siber di IoV sangat tinggi, maka skor dari penelitian sebelumnya masih perlu ditingkatkan lagi hingga mencapai keberhasilan 100%. Oleh karena itu, penelitian ini fokus pada upaya meningkatkan skor akurasi dan F1-Score dalam deteksi serangan siber pada IoV dengan menggunakan algoritma kNN.

METODE

Tahapan penelitian ini meliputi: pengumpulan data, pre-processing, pemodelan, dan evaluasi (Gambar 1).



Gambar 1. Tahapan penelitian

Hardware dan Software

Perangkat keras (*hardware*) dan perangkat lunak (*software*) memiliki peran krusial dalam mendukung kelancaran dan keberhasilan pelaksanaan penelitian (Rafrastara *et al.*, 2023). Jumlah data yang diolah pada penelitian ini adalah lebih dari 1 juta *records*, sehingga membutuhkan *hardware* dan *software* yang tepat. Berikut ini adalah spesifikasi *hardware* yang digunakan pada penelitian ini:

- Processor : Intel Xeon E5620
- RAM : 16 GB
- HD : 3 TB
- VGA : Radeon RX550

Software yang digunakan dalam eksperimen pada penelitian ini adalah Orange Data Mining, yaitu *software* berbasis *open source* yang mendukung pemrograman visual untuk kegiatan data mining. Orange dapat didownload di https://orangedatamining.com.

Pengumpulan Data

Mengingat pola serangan di dunia siber terus mengalami perkembangan, maka kebaruan dataset menjadi krusial. Dataset yang digunakan pada penelitian ini merupakan dataset publik yang dikembangkan oleh para peneliti dari University of New Brunswick, Kanada, pada tahun 2024 (University of New Brunswick, 2024). Dataset tersebut bernama "CIC IoV Dataset 2024" (University of New Brunswick, 2024). Tabel 1 menunjukkan detail spefisikasi dari dataset yang digunakan.

Data IoV yang digunakan pada penelitain ini merupakan data *On-board*, yaitu data yang digunakan untuk memonitor status perangkat pada kendaraan, seperti gas/akselerator, sistem pengereman, kemudi, *velocity*, *Revolutions per Minute (RPM)*, kecepatan, dan beberapa parameter lainnya (Sherazi *et al.*, 2019). Karena data yang digunakan adalah data on-board, maka serangannya pun juga serangan *on-board*, seperti *Denial of Service (DoS)*, *gas-spoofing, steering wheel-spoofing, speed, spoofing,* dan *RPM-spoofing*.

Tabel 1. Informasi dataset yang digunakan.

Nama Dataset	CIC IoV Dataset 2024
Tahun Pembuatan	2024
Jumlah Fitur	11
Jumlah Instances	1.408.249
Jumlah Kelas	6 (Benign, DoS, Gas-Spoofing, Steering Wheel-Spoofing, Speed-Spoofing, dan RPM-Spoofing)

Pra-Pemrosesan

Tahap *pre-processing* atau pra-pemrosesan merupakan tahap menyiapkan data dari data mentah (*raw data*) menjadi data yang siap untuk digunakan dalam pemodelan. Pada tahap ini, dilakukanr reduksi fitur dengan menghapus beberapa fitur yang tidak relevan, seperti ID, label, dan category. Dengan demikian, jumlah fitur yang tersisa adalah sebanyak 8 fitur, yaitu DATA_0, DATA_1, DATA_2, DATA_3, DATA_4, DATA_5, DATA_6, dan DATA_7.

DATA_0 merupakan isi byte pertama pada data yang ditransmisikan, sedangkan DATA_7 merupakan isi byte terakhirnya. Mengingat panjang payload yang dibawa oleh setiap *dataframe* pada protokol *CAN (Controller Area Network)* berukuran 8 byte, maka data-data yang dikirim tersebut dapat dipecah menjadi 8 bagian dan dijadikan sebagai fitur (DATA_0 hingga DATA_7).

Pemodelan

Tahap pemodelan merupakan tahap implementasi algoritma machine learning untuk mendapatkan model yang digunakan untuk melakukan klasifikasi, regresi, klasterisasi ataupun asosiasi. Pada tahap pemodelan ini, algoritma k-Nearest Neighbor (kNN) diimplementasikan guna mengklasifikasi data, apakah tergolong trafik yang normal *(benign)*, serangan DoS, atau serangan spoofing (*gas-spoofing, steering wheel-spoofing, speed, spoofing,* dan *RPM-spoofing*).

Algoritma k-Nearest Neighbors (kNN) merupakan metode supervised learning yang dapat digunakan untuk melakukan tugas klasifikasi dan regresi. kNN bekerja dengan cara menghitung jarak antara objek baru dengan setiap objek dalam data pelatihan (*training set*). Jarak tersebut dihitung dengan menggunakan metode pengukuran jarak, beberapa diantaranya yaitu: Euclidean, Manhattan, dan Chebyshev (Rafrastara *et al.*, 2024). Objek tersebut diklasifikasikan berdasarkan mayoritas dari sejumlah *k* tetangga terdekatnya. Jika menggunakan k = 5, kemudian mayoritas dari 5 tetangga terdekatnya tersebut merupakan kelas X, maka objek baru akan diklasifikasikan sebagai kelas X juga.

kNN merupakan algoritma yang sederhana dan mudah diimplementasikan. Algoritma kNN memiliki keunggulan yaitu memiliki performa yang efektif pada data berdimensi rendah hingga sedang. Oleh karena itu, algoritma ini cocok digunakan pada dataset CIC IoV Dataset 2024 mengingat jumlah fitur yang digunakan hanyalah 8 fitur (setelah reduksi).

Algoritma kNN masuk kategori lazy learner mengingat algoritma ini tidak menggunakan data pelatihan untuk melakukan generalisasi. kNN tidak memiliki fase pelatihan (*training*) secara eksplisit, karena proses *training* dilakukan saat fase prediksi atau pengujian sekaligus (Rafrastara *et al.*, 2024).

Tahapan dalam algoritma kNN adalah sebagai berikut (Supriyanto *et al.*, 2024):

1. Memilih nilai k.
2. Menghitung jarak antara data atau objek baru dengan semua objek.
3. Mengurutkan hasil pengukuran jarak secara ascending.
4. Memilih sejumlah k objek yang memiliki jarak terkecil.
5. Menghitung nilai modus (untuk klasifikasi) atau mean (untuk regresi) dari beberapa kelas objek yang dihasilkan pada nomor 4.

Pada penelitian ini, nilai k yang digunakan adalah k=5, dan metode pengukuran jarak yang digunakan adalah Euclidean Distance. Formula Euclidean Distance dapat dilihat pada Equation 1 (Supriyanto *et al.*, 2024).

$$d(p,q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2} \quad (1)$$

Dimana p dan q merupakan dua objek di dalam dataset.p merupakan objek *existing*, sementara q merujuk pada objek baru.

Evaluasi

Untuk mengukur performa algoritma kNN dalam mendeteksi serangan pada IoV, 2 metode pengukuran berbasis *Confusion Matrix* digunakan pada penelitian ini, yaitu Akurasi dan F1-Score. Namun sebelum dimulai pengukuran, perlu dilakukan validasi terlebih dahulu dengan memisahkan training dan testing set. Metode validasi yang digunakan adalah *Cross Validation*.

Cross Validation merupakan metode validasi dengan membagi dataset menjadi

beberapa bagian (*fold*) dan mengulangi proses pelatihan serta pengujian. Dalam metode *k-fold cross validation*, data dibagi menjadi k *fold*, dimana setiap *fold* bergantian menjadi set pengujian (*testing*), sementara yang lainnya digunakan sebagai set pelatihan (*training*). Proses ini membantu mengestimasi performa model secara lebih stabil dan menghindari *overfitting* (Battineni *et al.*, 2019; Orrù *et al.*, 2020). Pada penelitian ini, pemisahan data *training* dan *testing* dilakukan dengan *10-fold Cross Validation*.

Setelah dataset berhasil dipisahkan antara set pelatihan dan pengujian, maka pengukuran performa dilakukan dengan terlebih dahulu mengerjakan *Confusion Matrix*-nya. *Confusion Matrix* merupakan sebuah *matrix* yang dapat secara visual memberikan gambaran performa suatu algoritma, khususnya algoritma *supervised learning*. *Confusion Matrix* memiliki 4 komponen, yaitu TP (*True Positive*), TN (*True Negative*), FP (*False Positive*), dan FN (*False Negative*). Ilustrasi tabel Confuion Matrix dapat dilihat pada Tabel 2.

Tabel 2. Confusion Matrix

Classification		**Actual Class**	
		Positive	**Negative**
Prediction Class	**Positive**	TP	FP
	Negative	FN	TN

TP merupakan jumlah data positif yang benar-benar diklasifikasikan dengan benar oleh model. TN merupakan jumlah data negatif yang benar-benar diklasifikasikan dengan benar oleh model. FP merupakan jumlah data negatif yang salah diklasifikasikan sebagai positif oleh model. Sedangkan FN merupakan jumlah data positif yang salah diklasifikasikan sebagai negatif oleh model. Dengan mengetahui nilai TP, TN, FP, dan FN, maka skor akurasi dapat dihitung dengan menggunakan formula seperti pada Equation 2. Akurasi merupakan metrik untuk mengukur seberapa sering suatu model memprediksi dengan tepat (Dev *et al.*, 2022).

$$Accuracy = \frac{TP+TN}{(TP+FP+TN+FN)} \quad (2)$$

Metrik evaluasi kedua yang digunakan yaitu *F1-Score* (Equation 3). Metrik ini berguna untuk memperoleh nilai keseimbangan antara Presisi dan *Recall* (Gupta, Rai and Jha, 2021). Presisi merupakan metrik untuk mengukur seberapa banyak dari hasil positif yang benar-benar relevan (Equation 4). Sedangkan *Recall* yaitu metrik untuk mengukur seberapa banyak dari keseluruhan data positif yang berhasil ditemukan oleh model (Equation 5).

$$F1\ Score = \frac{2x(Precision\ x\ Recall)}{Precision+Recall} \quad (3)$$

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

$$Recall = \frac{TP}{TP+FN} \quad (5)$$

HASIL DAN PEMBAHASAN

Dataset yang digunakan adalah "CIC IoV 2024" yang terdiri dari 12 kolom dan 1.408.249 baris. Salah satu kolom bernama *specific_class* dijadikan sebagai *target class* karena berisi label-label pengklasifikasian. Sedangkan 11 kolom sisanya dijadikan sebagai fitur.

Pada tahap pre-processing, dilakukan reduksi fitur, yaitu dengan membuang fitur-fitur yang dinilai tidak relevan dan tidak memiliki korelasi dengan kelas target. Terdapat 3 fitur yang dihapus, yaitu *ID*, *label*, dan *category*. Dengan demikian, tersisa 8 fitur yang siap digunakan pada tahap pemodelan.

Pada tahap pemodelan, algoritma kNN diimplementasikan dengan k=5 dan Euclidean Distance sebagai metode pengukuran jaraknya. Setelah divalidasi menggunakan 10-fold Cross Validation, performa yang didapatkan oleh algoritma kNN dalam mendeteksi serangan pada IoV terlihat pada Tabel 3.

Tabel 3. Hasil performa algoritma kNN

Akurasi	**Recall**	**Presisi**	**F1-Score**
98.7%	98.7%	98.9%	98.7%

Performa akurasi dari algoritma kNN adalah 98.7%, recall 98.7%, presisi 98.9%, dan F1-Score 98.7%. Pada penelitian ini, terdapat 2 metrik yang difokuskan, yaitu Akurasi dan F1-Score. Metrik akurasi memiliki peran untuk mengetahui seberapa sering model memprediksi dengan tepat. Sedangkan metrik *F1-Score* dipilih karena *false positive* dan *false negative* memiliki resiko yang sama besarnya. Oleh karena itu, keseimbangan antara presisi dan *recall* dapat diperoleh dengan menggunakan metrik *F1-Score*.

Untuk mengetahui efektifitas algoritma kNN dibandingkan dengan algoritma-algoritma

lain, Tabel 4 memuat hasil perbandingan antara algoritma kNN dan 3 algoritma lain.

Tabel 4. Hasil perbandingan algoritma kNN dengan *state-of-the-arts*

Algoritma	Akurasi	F1-Score
kNN *(proposed)*	98.7%	98.7%
Naive Bayes (Rafrastara, Ghozi and Wardoyo, 2024)	98.1%	98.1%
Deep Neural Network (Neto *et al.*, 2024)	96.0%	78.0%
Random Forest (Neto *et al.*, 2024)	96.0%	76.0%

Hasilnya, kNN mengungguli algoritma Naive Bayes, Deep Neural Network, sekaligus Random Forest. Skor akurasi yang didapatkan oleh kNN yaitu sebesar 98.7% dan untuk metrik F1-Score juga memperoleh skor 98.7%. Skor yang diperoleh kNN lebih tinggi 0.6% dibandingkan dengan algoritma Naive Bayes yang diusulkan oleh (Rafrastara, Ghozi and Wardoyo, 2024). kNN juga mengungguli 2 algoritma yang digunakan pada paper (Neto *et al.*, 2024), yaitu Random Forest dan Deep Neural Network, dimana keduanya memiliki skor akurasi 96.0% dan F1-Score di bawah 80%. Hasil tersebut menunjukkan bahwa algoritma kNN terbukti lebih efektif dibandingkan dengan 3 algoritma yang lain, yaitu Naive Bayes, Deep Neural Network, dan Random Forest.

SIMPULAN

Penggunaan teknologi internet pada IoV dapat meningkatkan potensi serangan siber, seperti Denial of Service (DoS) dan Spoofing. Intrusion Detection System pada IoV belum sepenuhnya berjalan dengan baik mengingat teknologi IoV juga tergolong baru. Tujuan penelitian ini yaitu untuk mengevaluasi performa algoritma machine learning k-Nearest Neighbor (kNN) dalam mendeteksi serangan siber pada IoV. Dataset yang digunakan adalah dataset publik bernama CIC IoV2024 dataset decimal. Hasilnya, k-Nearest Neighbor (kNN) mendapatkan performa dengan skor 98.7% untuk metrik akurasi maupun F1-Score. kNN juga mengungguli 3 algoritma lain sebagai *state-of-the-arts*, yaitu Naïve Bayes (akurasi & F1-Score sebesar 98.1%), Deep Neural Network (akurasi: 96% & F1-Score: 78.0%), dan Random Forest (akurasi: 96% & F1-Score: 76.0%). Dengan demikian, algoritma kNN dapat direkomendasikan sebagai alternatif classifier dalam pengembangan intrusion detection system pada IoV.

Dataset CIC IoV 2024 terbagi menjadi dua tipe bilangan yaitu biner dan decimal. Penelitian ini berfokus pada dataset decimal, maka kami memberikan saran untuk mengembangkan deteksi serangan dengan dataset biner pada penelitian mendatang.

DAFTAR PUSTAKA

Ahmed, I., Jeon, G. and Ahmad, A. (2023) 'Deep Learning-Based Intrusion Detection System for Internet of Vehicles', *IEEE Consumer Electronics Magazine*, 12(1), pp. 117–123. Available at: https://doi.org/10.1109/MCE.2021.3139170.

Battineni, G. *et al.* (2019) 'Comparative Machine-Learning Approach: A Follow-Up Study on Type 2 Diabetes Predictions by Cross-Validation Methods', *Machines*, 7(4), p. 74. Available at: https://doi.org/10.3390/machines7040074.

Chen, M. *et al.* (2024) 'An attribute-encryption-based cross-chain model in urban internet of vehicles', *Computers and Electrical Engineering*, 115, p. 109136. Available at: https://doi.org/10.1016/j.compeleceng.2024.109136.

Chung, W. and Cho, T. (2022) 'Complex attack detection scheme using history trajectory in internet of vehicles', *Egyptian Informatics Journal*, 23(3), pp. 499–510. Available at: https://doi.org/10.1016/j.eij.2022.05.002.

Dev, S. *et al.* (2022) 'Performance Analysis and Prediction of Diabetes using Various Machine Learning Algorithms', in *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*. *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, Greater Noida, India: IEEE, pp. 517–521. Available at: https://doi.org/10.1109/ICAC3N56670.2022.10074117.

Djenouri, Y. *et al.* (2024) 'Enhancing smart road safety with federated learning for Near Crash Detection to advance the

development of the Internet of Vehicles', *Engineering Applications of Artificial Intelligence*, 133, p. 108350. Available at: https://doi.org/10.1016/j.engappai.2024.108350.

Gupta, G., Rai, A. and Jha, V. (2021) 'Predicting the Bandwidth Requests in XG-PON System using Ensemble Learning', in *2021 International Conference on Information and Communication Technology Convergence (ICTC)*. *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea, Republic of: IEEE, pp. 936–941. Available at: https://doi.org/10.1109/ICTC52510.2021.9620935.

Haodudin Nurkifli, E. and Hwang, T. (2023) 'Provably secure authentication for the internet of vehicles', *Journal of King Saud University - Computer and Information Sciences*, 35(8), p. 101721. Available at: https://doi.org/10.1016/j.jksuci.2023.101721.

Islam, S. *et al.* (2022) 'State-of-the-art vehicle-to-everything mode of operation of electric vehicles and its future perspectives', *Renewable and Sustainable Energy Reviews*, 166, p. 112574. Available at: https://doi.org/10.1016/j.rser.2022.112574.

Kaur, G. and Garg, H. (2023) 'A novel algorithm for autonomous parking vehicles using adjustable probabilistic neutrosophic hesitant fuzzy set features', *Expert Systems with Applications*, 226, p. 120101. Available at: https://doi.org/10.1016/j.eswa.2023.120101.

Korium, M.S. *et al.* (2024) 'Intrusion detection system for cyberattacks in the Internet of Vehicles environment', *Ad Hoc Networks*, 153, p. 103330. Available at: https://doi.org/10.1016/j.adhoc.2023.103330.

Neto, E.C.P. *et al.* (2024) 'CICIoV2024: Advancing realistic IDS approaches against DoS and spoofing attack in IoV CAN bus', *Internet of Things*, 26, p. 101209. Available at: https://doi.org/10.1016/j.iot.2024.101209.

Orrù, G. *et al.* (2020) 'Machine Learning in Psychometrics and Psychological Research', *Frontiers in Psychology*, 10, p. 2970. Available at: https://doi.org/10.3389/fpsyg.2019.02970.

Qureshi, K.N. *et al.* (2021) 'Internet of Vehicles: Key Technologies, Network Model, Solutions and Challenges With Future Aspects', *IEEE Transactions on Intelligent Transportation Systems*, 22(3), pp. 1777–1786. Available at: https://doi.org/10.1109/TITS.2020.2994972.

Rafrastara, F.A. *et al.* (2023) 'Deteksi Malware menggunakan Metode Stacking berbasis Ensemble', *Jurnal Informatika*, 8(1), pp. 11–16.

Rafrastara, F.A. *et al.* (2024) 'Performance Comparison of k-Nearest Neighbor Algorithm with Various k Values and Distance Metrics for Malware Detection', 8.

Rafrastara, F.A., Ghozi, W. and Wardoyo, A. (2024) 'Deteksi Serangan berbasis Machine Learning pada Internet of Vehicle', in *IN-FEST 2024*. *IN-FEST 2024: Seminar Nasional Informatika - FTI UPGRIS*, UPGRIS Semarang: UPGRIS Semarang.

Sherazi, H.H.R. *et al.* (2019) 'DDoS attack detection: A key enabler for sustainable communication in internet of vehicles', *Sustainable Computing: Informatics and Systems*, 23, pp. 13–20. Available at: https://doi.org/10.1016/j.suscom.2019.05.002.

Supriyanto, C. *et al.* (2024) 'Malware Detection Using K-Nearest Neighbor Algorithm and Feature Selection', 8.

University of New Brunswick (2024) 'CIC IoV dataset 2024: Advancing Realistic IDS Approaches against DoS and Spoofing Attack in IoV CAN bus'. Available at: https://www.unb.ca/cic/datasets/iov-dataset-2024.html (Accessed: 9 June 2024).

Wang, M. and Wang, S. (2021) 'Communication Technology and Application in Internet of Vehicles', in *2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE)*. *2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE)*, Dalian, China: IEEE, pp. 234–237. Available at:

https://doi.org/10.1109/ICISCAE52414.2021.9590660.

Wei, X. (2024) 'Enhancing road safety in internet of vehicles using deep learning approach for real-time accident prediction and prevention', *International Journal of Intelligent Networks*, 5, pp. 212–223. Available at: https://doi.org/10.1016/j.ijin.2024.05.002.