DETEKSI SERANGAN *DISTRIBUTED DENIAL OF SERVICE* PADA PROTOKOL COAP (*CONSTRAINED APPLICATION PROTOCOL*) IOT MENGGUNAKAN *SUPPORT VECTOR MACHINE*

USULAN SKRIPSI

Oleh :

SHOLIKIN

NIM. 200605110119

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM

MALANG

2024

LEMBAR PERSETUJUAN

USULAN SKRIPSI

DETEKSI SERANGAN DISTRIBUTED DENIAL OF SERVICE PADA PROTOKOL COAP (CONSTRAINED APPLICATION PROTOCOL) IOT MENGGUNAKAN SUPPORT VECTOR MACHINE

Oleh :

SHOLIKIN

NIM. 200605110119

Telah Diperiksa dan Disetujui untuk Diuji:
Tanggal: Maret 2024

Pembimbing I,	Yang Mengajukan,
Johan Ericka Wahyu Prakasa, M.Kom	Sholikin
NIP. 198312132019031004	NIM. 200605110119

DAFTAR ISI

BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi telah membuka era baru dalam cara manusia berinteraksi dengan lingkungan di sekitarnya, terutama dengan kehadiran *Internet of Things* (IoT). Melalui IoT, berbagai perangkat dapat terhubung dengan internet, memungkinkan pertukaran data dan kontrol yang lebih efisien. Namun, seiring perkembangan ini, muncul tantangan baru mengenai keamanan dan privasi yang perlu diperhatikan. Keamanan jaringan merupakan elemen yang sangat penting khususnya dalam jaringan IoT (Fibrianda & Bhawiyuga, 2018).

Salah satu protokol komunikasi yang umum digunakan dalam IoT adalah *Constrained Application Protocol* (CoAP). Protokol ini dirancang untuk beroperasi pada perangkat dengan sumber daya terbatas, seperti sensor kecil atau perangkat *wearable*, sehingga lebih efisien dalam penggunaan sumber daya (Almeghlef et al., 2023). Karena digunakan pada perangkat dengan sumber daya terbatas, membuatnya menjadi target yang menarik bagi serangan Distributed *Denial of Service* (DDoS) yang bertujuan membuat layanan tidak tersedia bagi pengguna dengan membanjiri sumber daya jaringan (Maulana, 2023).

Melansir dari laman https://blog.cloudflare.com/ddos-threat-report-2023-q3. Pada pada kuartal 3 tahun 2023, terjadi peningkatan serangan DDoS sebesar 65% dibandingkan dengan kuartal sebelumnya. Totalnya, tercatat sebanyak 8,9 triliun permintaan HTTP DDoS yang berhasil dideteksi dan ditangani secara

otomatis oleh sistem *Cloudflare*. Selain itu, secara keseluruhan pada Q3, serangan DDoS yang mengeksploitasi *Constrained Application Protocol* (CoAP) menduduki peringkat kedua setelah serangan berbasis *Multicast* DNS (mDNS).

[CoAP-Report] dan [CoAP-Wild] melaporkan faktor amplifikasi rata-rata sebesar 27 dan 34 masing-masing dari satu respons terhadap permintaan GET untuk /.well-dikenal/inti ke port UDP default 5693 (Mattsson et al., 2022). *Cloudflare* juga melaporkan bahwa serangan DDoS CoAP mengalami peningkatan mencolok sebesar 387%. *Constrained Application Protocol* (CoAP) pada dasarnya dirancang untuk digunakan dalam komunikasi antar perangkat dengan daya rendah dan ringan. Namun, hal ini disalahgunakan untuk serangan DDoS. Para pelaku kejahatan memanfaatkan fitur-fitur *multicast* dari CoAP yang tidak terlindungi dengan baik untuk menghasilkan lalu lintas jaringan yang besar dan merugikan (Rachit et al., 2021).

Hal ini tentunya akan sangat merugikan karena ketika perangkat IoT menjadi target serangan DDoS, maka layanan yang bergantung pada perangkat akan terganggu atau bahkan tidak tersedia sama sekali. Akibatnya, pengguna tidak dapat mengakses atau mengendalikan perangkat, sehingga menyebabkan kerugian finansial, kerugian reputasi, dan dapat mengganggu kegiatan sehari-hari yang terkait dengan layanan yang terganggu.

Sebagaimana dalam AL-Qur’an Surah Al A’raf ayat 56

وَلَا تُفْسِدُوا فِي الْأَرْضِ بَعْدَ إِصْلَاحِهَا وَادْعُوهُ خَوْفًا وَطَمَعًا ۚ إِنَّ رَحْمَتَ اللَّهِ قَرِيبٌ مِنَ الْمُحْسِنِينَ

Dan janganlah kamu berbuat kerusakan di bumi setelah (diciptakan) dengan baik. Berdoalah kepada-Nya dengan rasa takut dan penuh harap. Sesungguhnya rahmat Allah sangat dekat kepada orang yang berbuat kebaikan. (QS. Surat Al A'raf:56)

DDoS merupakan tindakan yang merusak dan dilarang oleh Al-Qur'an. Ayat ini menegaskan larangan berbuat segala bentuk kerusakan atau kerugian yang dapat menimbulkan kebinasaan. Serangan DDoS, dengan dampaknya yang merusak layanan dan sumber daya, dapat dilihat sebagai salah satu bentuk berbuat kerusakan di muka bumi. Oleh karena itu, ayat ini mengingatkan kita untuk tidak menyebabkan kerusakan atau kehancuran, tetapi sebaliknya, untuk berusaha melakukan kebaikan dan menjaga stabilitas dalam segala hal, termasuk dalam penggunaan teknologi dan layanan yang kita gunakan.

Penelitian ini bertujuan untuk mendeteksi serangan DDoS yang terjadi pada protokol COAP menggunakan algoritma *Support Vector Machine* (SVM). Pemilihan SVM didasarkan pada keunggulannya dalam mengatasi masalah overfitting dan popularitasnya dalam deteksi serangan (Sihombing et al., 2019). Dalam penelitian mereka mengidentifikasi serangan DDoS dengan tingkat akurasi mencapai 96,83%, dan waktu deteksinya berkisar sekitar 67,80 milidetik. Sementara itu pada penelitian lainnya dalam mendeteksi searangan DDoS menggunakan *Support Vector Machine* menghasilkan akurasi sebesar 98,37% (Maulana, 2023). SVM cocok digunakan dalam masalah klasifikasi biner atau multi-kelas, serta mampu bekerja baik dalam kasus di mana ada pemisah *linier* atau *non-linier* yang jelas antara kelas (Sihombing et al., 2019). Deteksi serangan

DDoS sangat penting dalam menjaga ketersediaan layanan dan keamanan data dalam lingkungan IoT yang rentan terhadap serangan.

1.2 Rumusan Masalah

Bagaimana mengidentifikasi *traffic* serangan DDoS pada jaringan IoT yang menggunakan protokol CoAP dengan Algoritma *Support Vector Machine*?

1.3 Batasan Masalah

a. Data yang digunakan merupakan data *traffic* serangan DDoS dan *non*-DDoS pada protokol CoAP yang didapatkan dari Kaggle dengan judul "DDoS CoAP dataset (CIDAD)".
b. Fokus penelitian ini hanya pada deteksi *traffic* serangan DDoS dan *non*-DDoS pada protokol CoAP.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini ialah untuk mengidentifikasi *traffic* serangan *Distributed Denial of Service* (DDoS) yang ditargetkan pada protokol *Constrained Application Protocol* (CoAP) dalam jaringan *Internet of Things* (IoT) menggunakan algoritma *Support Vector Machine*.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memiliki peran penting dalam meningkatkan keamanan jaringan IoT, khususnya pada protokol CoAP dari serangan DDoS, yang dapat membantu industri dan penyedia layanan IoT mengembangkan sistem keamanan yang lebih kuat dan efektif.

<<Atau brntuk List>>

BAB II
STUDI PUSTAKA

2.1 Penelitian Terdahulu

Penelitian yang dilakukan oleh Tedyyana dan rekan-rekannya mengusulkan metode inovatif dalam meningkatkan keamanan server web melalui penerapan Sistem Deteksi Intrusi yang diperkuat dengan algoritma *Machine Learning*. Penelitian ini menggunakan dataset publik yang transparan dan melalui serangkaian proses pra-pemrosesan data yang intensif, termasuk pembersihan, normalisasi, dan pemilihan fitur. Hasilnya, algoritma pembelajaran mesin mampu membedakan ancaman siber potensial dari pola standar dengan lebih baik daripada sistem deteksi intrusi tradisional yang tanpa algoritma pembelajaran. Penelitian ini menunjukkan peningkatan signifikan dalam akurasi model dan pengurangan alarm palsu, yang memperkuat argumen akan manfaat penggunaan pembelajaran mesin dalam meningkatkan keamanan siber. Studi ini juga memberikan landasan untuk penelitian lebih lanjut tentang mekanisme perlindungan yang lebih baik kedepanya (Tedyyana et al., 2024).

Sementara penelitian yang dilakukan oleh (Lami & Pella, 2022)mengenalkan sistem hibrida yang didasarkan pada teknik klasifikasi terawasi untuk mendeteksi serangan *Denial of Service* (DoS) pada jaringan *Internet of Things* (IoT) yang menggunakan protokol CoAP. Validasi sistem dilakukan menggunakan dataset yang mencakup lalu lintas jaringan dari jaringan IoT yang mengalami serangan DoS. Hasil dari penelitian menunjukkan bahwa sistem yang diusulkan berhasil mendeteksi serangan DoS pada jaringan IoT

melalui protokol CoAP menggunakan teknik klasifikasi terawasi. Dataset yang digunakan untuk validasi sistem ini merupakan lalu lintas jaringan dari jaringan IoT yang telah mengalami serangan DoS (Lami & Pella, 2022).

Penelitian sebelumnya yang dilakukan oleh Granjal dan rekan-rekanya mengusulkan implementasi dan evaluasi deteksi intrusi berbasis anomali, khususnya untuk serangan Denial of Service (DoS) dan serangan terhadap protokol komunikasi 6LoWPAN dan CoAP. Algoritma *Support Vector Machine* (SVM) digunakan pada penelitian ini, dengan parameter SVM yang dikaji meliputi tipe kernel (*linear*, RBF, *polinomial*, *sigmoidal*) dan metrik penilaian (akurasi). Hasilnya pendekatan yang diusulkan dapat efektif melindungi perangkat dari serangan, dengan mencapai akurasi sebesar 93% untuk masalah multi-kelas dan 92% untuk masalah kelas biner (Granjal et al., 2018).

Pada penelitian yang dilakukan oleh Maulana pada tahun 2023, beberapa model algoritma *machine learning* diterapkan untuk mendeteksi serangan DDoS pada arsitektur *Software Defined Network* (SDN) diantaranya ialah *random forest, support vector machine, K-nearest neighbor, dan multi-layer perceptron*. Hasil penelitian menunjukkan bahwa algoritma *random forest* mencapai akurasi tertinggi sebesar 99.41%, diikuti oleh *K-nearest neighbor* dengan akurasi 99%, *support vector machine* dengan akurasi 98.37%, dan multi-layer perceptron dengan akurasi 93.97%. (Maulana, 2023).

Penelitian dengan membandingkan akurasi deteksi serangan pada jaringan komputer menggunakan metode *Naïve Bayes* dan *Support Vector Machine* (SVM) dilakukan oleh Fibrianda & Bhawiyuga. Dalam penelitian ini, metode *Naïve*

Bayes dan beberapa varian SVM (*Linear, Polynomial, dan Sigmoid*) digunakan untuk melakukan analisis perbandingan. Persentase akurasi yang dihasilkan dari proses klasifikasi adalah sebagai berikut: *Naïve Bayes* (85,055%), SVM *Linear* (99,995%), SVM *Polynomial* (99,999%), dan SVM *Sigmoid* (99,995%). Dari hasil ini, SVM *Polynomial* menunjukkan persentase akurasi tertinggi, sementara Naïve Bayes memiliki persentase akurasi terendah. Ini menunjukkan bahwa SVM *Polynomial* dapat dianggap sebagai metode yang lebih unggul dalam deteksi serangan pada jaringan komputer dibandingkan dengan *Naïve Bayes* (Fibrianda & Bhawiyuga, 2018).

2.2 Protokol *Constrained Application Protocol* (CoAP)

Constrained Application Protocol (CoAP) adalah sebuah protokol komunikasi pada jaringan *Internet of Things* (IoT) yang dirancang untuk mendukung interaksi efisien antara perangkat IoT yang memiliki keterbatasan sumber daya. Protokol ini menggunakan model *RESTful* dan berjalan di atas protokol UDP untuk mengoptimalkan penggunaan bandwidth dan energi (Mattsson et al., 2024). CoAP pertama kali didefinisikan dalam RFC 7252 pada bulan Juni 2014 oleh C. Bormann dan Z. Shelby. Sejak itu, CoAP telah menjadi salah satu protokol komunikasi yang populer dalam implementasi IoT (Mattsson et al., 2024).

CoAP memberikan cara yang sederhana untuk merespons permintaan akses dan pengelolaan sumber daya. Protokol ini mendukung berbagai metode seperti GET, POST, PUT, dan DELETE untuk berinteraksi dengan sumber daya.

CoAP juga memiliki fitur seperti opsi observasi untuk memantau sumber daya dan transfer blok untuk menangani data yang besar. Kelebihan CoAP meliputi pengurangan penundaan, penghematan energi, dan pengurangan kompleksitas dibandingkan dengan HTTP. Protokol ini dapat digunakan dengan infrastruktur dan jaringan yang sudah ada, sehingga sangat sesuai untuk aplikasi IoT (Seoane et al., 2021).

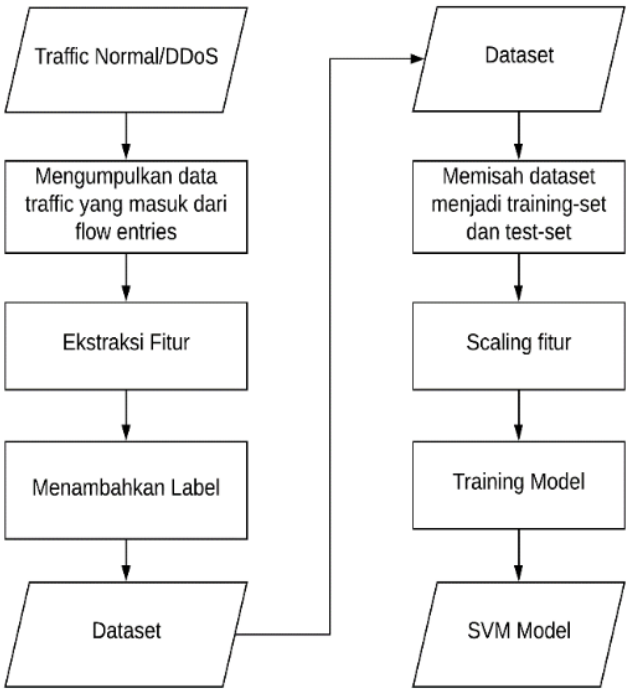
Penelitian yang dilakukan oleh Seoane bertujuan untuk menganalisis kinerja dua protokol yang paling populer untuk lapisan aplikasi dalam jaringan Internet of Things (IoT), yaitu *Constrained Application Protocol* (CoAP) dan *Message Queue Telemetry Transport* (MQTT). Analisis difokuskan pada kemampuan operasional protokol di bawah kendala perangkat terbatas, dengan mempertimbangkan aspek keamanan dan variasi kondisi jaringan. Hasil analisis menunjukkan bahwa CoAP dan MQTT memiliki kelebihan dan kelemahan masing-masing dalam beroperasi di bawah kendala perangkat terbatas. (Seoane et al., 2021).

Berdasarkan penelitian diatas, CoAP dirancang khusus untuk perangkat dengan sumber daya terbatas dan juga berjalan diatas protokol UDP yang mana memiliki *overhead* yang lebih rendah dan lebih ringan dibandingkan MQTT yang menggunakan protokol TCP. CoAP mengurangi penundaan transmisi data dengan menggunakan *header* ringkas, seperti yang dilakukan HTTP. CoAP mampu meminimalkan konsumsi daya dan overhead, menjadikannya ideal untuk perangkat IoT dengan sumber daya terbatas (Seoane et al., 2021).

2.3 *Support Vector Machine* (SVM)

Support Vector Machine (SVM) adalah algoritma *Machine Learning* yang biasa digunakan untuk proses klasifikasi. SVM beroperasi dengan cara menemukan *hyperplane* optimal yang memisahkan antara dua kelas dalam ruang fitur sedemikian rupa sehingga jarak antara *hyperplane* dan *instance* terdekat dari masing-masing kelas (yang disebut sebagai *support vectors*) adalah maksimum. Dengan kata lain, SVM bertujuan untuk mencari *hyperplane* dengan margin terbesar yang memisahkan data dengan baik (Suprihadi & Magfira, 2024).

Support Vector Machine (SVM) bekerja dengan memetakan data input ke dalam ruang fitur dengan dimensi yang lebih tinggi, dimana *hyperplane* dapat digambarkan sebagai pembatas yang memisahkan dua kelas. SVM kemudian mencari *hyperplane* ini dengan memaksimalkan margin, yaitu jarak antara hyperplane dan titik terdekat dari masing-masing kelas (*support vectors*). Proses optimasi ini dilakukan dengan memformulasikan masalah sebagai masalah pembatasan (constraint) dan menyelesaikannya menggunakan teknik optimasi, seperti metode pembatasan *Lagrange*. SVM juga mampu menangani kasus di mana data tidak dapat dipisahkan secara linear di ruang fitur asli dengan menggunakan kernel trick, yang memungkinkan transformasi non-linear data ke dimensi yang lebih tinggi di mana pemisahan linear dapat dilakukan. Dengan demikian, SVM adalah algoritma unggul yang dapat digunakan untuk klasifikasi (Sihombing et al., 2019).



Gambar 1.1. Alur *Support Vector Machine*

Keunggulan SVM termasuk kemampuannya untuk menangani data dengan dimensi tinggi, dapat bekerja efisien dengan jumlah sampel yang lebih kecil, dan dapat menangani dataset yang tidak terstruktur dengan baik. SVM juga memiliki fleksibilitas dalam menggunakan berbagai fungsi kernel, seperti linear, polinomial, radial basis function (RBF), dan lainnya, yang memungkinkan adaptasi dengan baik terhadap struktur data yang kompleks (Wiranda et al., 2022).

Dibawah adalah beberapa jenis kernel yang umum digunakan dalam SVM (Mohammadi et al., 2021), antara lain:

1. Kernel Linear: Kernel linear adalah kernel paling sederhana yang digunakan dalam SVM. Kernel ini menghasilkan pemetaan linear, di mana tidak ada

transformasi data yang dilakukan. Fungsi kernel linear cocok untuk kasus di mana data secara intrinsik dapat dipisahkan secara linear dalam ruang fitur asli.

2. Kernel Polinomial: Kernel polinomial melakukan transformasi data ke ruang fitur yang memiliki dimensi lebih tinggi menggunakan fungsi polinomial. Dalam kernel polinomial, kita dapat mengatur derajat polinomial, yang mengontrol kompleksitas pemetaan. Kernel polinomial berguna untuk menangani data yang memiliki pola non-linear yang dapat dijelaskan dengan polinomial.
3. Radial Basis Function (RBF) Kernel: RBF kernel (atau Gaussian kernel) merupakan kernel yang sangat umum digunakan dalam SVM. Kernel ini mentransformasikan data ke ruang fitur yang memiliki dimensi tak terbatas menggunakan fungsi Gaussian. RBF kernel memiliki dua parameter: γ (gamma), yang mengontrol lebar distribusi Gaussian, dan C, yang merupakan parameter penalti. RBF kernel efektif dalam menangani data yang tidak linier terpisah.
4. Kernel Sigmoid: Kernel sigmoid melakukan transformasi data ke ruang fitur yang memiliki dimensi lebih tinggi menggunakan fungsi sigmoid. Kernel ini cocok untuk kasus di mana data tidak dapat dipisahkan secara linear, tetapi memiliki batas keputusan yang non-linear.

Pada penelitian ini penulis menggunakan SVM karena kemampuannya untuk mengklasifikasikan dan menganalisis data yang terkait dengan serangan jaringan, seperti serangan DDoS yang unggul. Perbedaan dari penelitian-penelitian sebelumnya ialah pada penggunaan datasetnya, pada penellitian ini

pneliti menggunakan dataset dari kaggle dengan nama “DDoS CoAP (CIDAD)” yang berisi traffic jaringan normal dan DDoS. Pada beberapa penelitian terdahulu dapat disimpiulkan bahwa SVM memiliki nilai akurasi yang tinggi terhadap klasifikasi serangan pada jaringan IoT. Dengan kemampuan SVM dan kinerja yang baik dalam berbagai kasus, SVM telah menjadi salah satu algoritma *machine learning* yang populer dan sering digunakan dalam berbagai penelitian klasifikasi.

BAB III
DESAIN DAN IMPLEMENTASI

3.1 Desain Penelitian

3.2 Pengumpulan Data

3.3 Pre-Processing Data

3.4 Analisis Data Serangan DDoS

3.5 Pemilihan Fitur yang Relevan

3.6 Pembagian Data untuk Pelatihan dan Pengujian

3.7 Pelatihan Model SVM

3.8 Pengujian Model SVM

3.9 Analisis dan Perancangan

3.1.1 Analisis

3.10 Desain Sistem

Desain ekomendasiLorem ipsum dolor sit amet, consecteturadipiscingelit, sed do eiusmodtemporincididuntutlabore et dolore magna aliqua. Euismod in pellentesquemassaplaceratduisultricieslacus.

Necsagittisaliquammalesuadabibendumarcu. Pellentesqueadipiscingcommodoelit at imperdiet dui accumsan. Congueeuconsequat ac felis. Sit ametmauriscommodoquis. Dolor purus non enimpraesentelementumfacilisisleo vel. Dignissimcrastinciduntlobortisfeugiatvivamus. Libero justolaoreet sit amet cursus sit amet dictum. A diam sollicitudintempor id eunisl. Elit pellentesque habitant morbitristiquesenectus et netus. Sed ullamcorpermorbitinciduntornaremassaegetegestas. Tortordignissim convallis

aenean et tortor at risusviverraadipiscing. Erat imperdiet sed euismod nisi porta lorem. Gravida dictum fusceutplacerat. Fermentum posuereurnanectinciduntpraesent semper feugiatnibh sed. Sed arcu non odioeuismod lacinia.

3.11Rancangan Perhitungan

n.Lorem ipsum dolor sit amet, consecteturadipiscingelit, sed do eiusmodtemporincididuntutlabore et dolore magna aliqua. Euismod in pellentesquemassaplaceratduisultricieslacus.

Necsagittisaliquammalesuadabibendumarcu. Pellentesqueadipiscingcommodoelit at imperdiet dui accumsan. Congueeuconsequat ac felis. Sit ametmauriscommodoquis. Dolor purus non enimpraesentelementumfacilisisleo vel. Dignissimcrastinciduntlobortisfeugiatvivamus. Libero justolaoreet sit amet cursus sit amet dictum. A diam sollicitudintempor id eunisl. Elit pellentesque habitant morbitristiquesenectus et netus. Sed ullamcorpermorbitinciduntornaremassaegetegestas. Tortordignissim convallis aenean et tortor at risusviverraadipiscing. Erat imperdiet sed euismod nisi porta lorem. Gravida dictum fusceutplacerat. Fermentum posuereurnanectinciduntpraesent semper feugiatnibh sed. Sed arcu non odioeuismod lacinia.

3.3.1 Desain PengujianSitem

. Lorem ipsum dolor sit amet, consecteturadipiscingelit, sed do eiusmodtemporincididuntutlabore et dolore magna aliqua. Euismod in pellentesquemassaplaceratduisultricieslacus.

Necsagittisaliquammalesuadabibendumarcu. Pellentesqueadipiscingcommodoelit at imperdiet dui accumsan. Congueeuconsequat ac felis. Sit ametmauriscommodoquis. Dolor purus non enimpraesentelementumfacilisisleo vel. Dignissimcrastinciduntlobortisfeugiatvivamus. Libero justolaoreet sit amet cursus sit amet dictum. A diam sollicitudintempor id eunisl. Elit pellentesque habitant morbitristiquesenectus et netus. Sed ullamcorpermorbitinciduntornaremassaegetegestas. Tortordignissim convallis aenean et tortor at risusviverraadipiscing. Erat imperdiet sed euismod nisi porta lorem. Gravida dictum fusceutplacerat. Fermentum posuereurnanectinciduntpraesent semper feugiatnibh sed. Sed arcu non odioeuismod lacinia.

DAFTAR PUSTAKA

Almeghlef, S. M., AL-Ghamdi, A. A.-M., Ramzan, M. S., & Ragab, M. (2023). Application Layer-Based Denial-of-Service Attacks Detection against IoT-CoAP. *Electronics*, *12*(12), 2563. https://doi.org/10.3390/electronics12122563

Fibrianda, M. F., & Bhawiyuga, A. (2018). Analisis Perbandingan Akurasi Deteksi Serangan Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan Support Vector Machine (SVM). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *2*(9), 3112–3123.

Granjal, J., Silva, J., & Lourenço, N. (2018). Intrusion Detection and Prevention in CoAP Wireless Sensor Networks Using Anomaly Detection. *Sensors*, *18*(8), 2445. https://doi.org/10.3390/s18082445

Lami, H. F. J., & Pella, S. I. (2022). *PERBANDINGAN UNJUK KERJA COAP DAN HTTP PADA TRANSAKSI DATA PERANGKAT IoT*. (2).

Mattsson, J. P., Fornehed, J., Selander, G., Palombini, F., & Amsüss, C. (2022, March 11). CoAP Attacks draft-mattsson-core-coap-attacks IETF 111. *Internet Engineering Task Force (IETF) Datatracker*.

Mattsson, J. P., Fornehed, J., Selander, G., Palombini, F., & Amsüss, C. (2024). *Attacks on the Constrained Application Protocol (CoAP)*. IETF Datatracker. Retrieved from https://datatracker.ietf.org/doc/draft-ietf-core-attacks-on-coap/

Maulana, I. (2023). Optimalisasi Deteksi Serangan DDoS Menggunakan Algoritma Random Forest, SVM, KNN dan MLP pada Jaringan Komputer. *ndonesian Journal of Mathematics and Natural Sciences*, *46*(2), 83–92.

Mohammadi, M., Rashid, T. A., Karim, S. H. T., Aldalwie, A. H. M., Tho, Q. T., Bidaki, M., … Hosseinzadeh, M. (2021). A comprehensive survey and taxonomy of the SVM-based intrusion detection systems. *Journal of Network and Computer Applications*, *178*, 102983. https://doi.org/10.1016/j.jnca.2021.102983

Rachit, Bhatt, S., & Ragiri, P. R. (2021). Security trends in Internet of Things: A survey. *SN Applied Sciences*, *3*(1), 121. https://doi.org/10.1007/s42452-021-04156-9

Seoane, V., Garcia-Rubio, C., Almenares, F., & Campo, C. (2021). Performance evaluation of CoAP and MQTT with security support for IoT environments. *Computer Networks*, *197*, 108338. https://doi.org/10.1016/j.comnet.2021.108338

Sihombing, J. C. J., Kartikasari, D. P., & Bhawiyuga, A. (2019). Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software-Defined Network (SDN). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *3*(10), 9608–9613.

Suprihadi, D., & Magfira, I. (2024). FORENSIK PADA JARINGAN KOMPUTER LOKAL DENGAN KLASIFIKASI SVM BERBASIS

FRAMEWORK TAARA. *Jurnal Review Pendidikan dan Pengajaran (JRPP)*, *7*(Nomor 1), 666.

Tedyyana, A., Ghazali, O., & Purbo, O. (2024). Model Design of Intrusion Detection System on Web Server Using Machine Learning Based. *Proceedings of the 11th International Applied Business and Engineering Conference, ABEC 2023, September 21st, 2023, Bengkalis, Riau, Indonesia*. Presented at the Proceedings of the 11th International Applied Business and Engineering Conference, ABEC 2023, September 21st, 2023, Bengkalis, Riau, Indonesia, Bengkalis, Indonesia. Bengkalis, Indonesia: EAI. https://doi.org/10.4108/eai.21-9-2023.2342879

Wiranda, N., Sadikin, F., & Saputra, W. A. (2022). Pembelajaran Mesin untuk Sistem Keamanan—Literatur Review. *IJEIS (Indonesian Journal of Electronics and Instrumentation Systems)*, *12*(1), 37. https://doi.org/10.22146/ijeis.69022