Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 153-162
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

Efektivitas Algoritma Cusum dalam Mendeteksi Serangan Denial of Service pada Trafik Jaringan Sensor Nirkabel

Taufik Hidayat, Nurhanif, Yeni Yanti*, Putri Nuri Pratama, Nadiatul Safana

Fakultas Teknik, Program Studi Teknik Komputer, Universitas Serambi Mekkah, Kota Banda Aceh, Indonesia
Email: [1]taufik.hidayat@serambimekkah.ac.id, [2]nurhanif@serambimekkah.ac.id, [3,*]yeniyanti@serambimekkah.ac.id,
[4]putrinuri0126@gmail.com, [5]nadiatulsafana415@gmail.com
Email Penulis Korespondensi: yeniyanti@serambimekkah.ac.id

Abstrak−Jaringan Sensor Nirkabel (JSN) dapat mengumpulkan dan mengirimkan informasi lingkungan secara real-time, dan fitur-fiturnya yang fleksibel dan efisien. Namun pada saat yang sama yang memiliki kelemahan daya yang terbatas, kemampuan pemrosesan yang rendah, keamanan,kepercayaan data, dan sangat rentang terhadap serangan terutama serangan Denial of Servis. Permasalahan yang dihadapi adalah meningkatnya risiko serangan Denial of Servis (DoS) yang mengganggu kinerja jaringan. Tujuan penelitian ini adalah untuk mengembangkan sistem deteksi yang dapat memantau dan mendeteksi serangan secara proaktif di Jaringan Sensor Nirkabel. Metode yang digunakan dalam penelitian ini meliputi pengumpulan data trafik dari dataset publik WSN-DS, dengan melakukan pengujian Trafik, Noise, Cusum. Untuk metode penelitian ini merepakan algoritma CUSUM. Hasil penelitian menunjukkan bahwa algoritma CUSUM mampu mendeteksi serangan DoS dengan tingkat akurasi mendekati 100%, Noise dataset DoS ($Data_R$) menghasilka noise sangat besar antara -1500 dan 1500, pola yang tidak stabil dari waktu ke waktu yang menunjukkan gangguan terbesar dibandingkan dataset ($Data_S$) dan dataset (ExpanedEnergy). Sedangkan untuk hasil Trafik dataset DoS ($Data_R$) menghasil nilai Volume Trafik lebih tinggi, berkisar antara 0 hingga 1500, dengan variasi signifikan. Terdapat fase di mana trafik menurun drastis atau berhenti, diikuti lonjakan besar, menunjukkan serangan yang lebih kuat dan intens pada periode tertentu.penelitian ini juga diharapkan dapat memperluaskan ilmu pengetahuan tentang teknik deteksi serangan untuk JSN.

Kata Kunci: Trafik; Noise; Algoritma Cusum; Jaringan Sensor Nirkabel; Serangan DoS;

1. PENDAHULUAN

Jaringan Sensor Nirkabel (JSN) telah berkembang pesat dalam beberapa tahun terakhir, dan telah menjadi salah satu bidang penting untuk penelitian dalam aplikasi jaringan (D. Liu et al., 2024). Biaya rendah dan kemudahan penyebarannya telah memungkinkannya untuk digunakan dalam berbagai perangkat sensor pintar seperti komunikasi dalam kendaraan, rumah pintar, dan pemantauan jarak jauh. Dengan perkembangan pesat dan penerapan perangkat jaringan sensor pintar yang meluas, banyak peneliti telah berfokus pada keamanan JSN (Zhao et al., 2021). JSN dapat mengumpulkan dan mengirimkan informasi lingkungan secara real-time, dan fitur-fiturnya yang fleksibel dan efisien. Namun pada saat yang sama, ia juga memiliki kelemahan daya yang terbatas, kemampuan pemrosesan yang rendah, keamanan, dan kepercayaan data (Mohammed & Misganaw, 2022), kekurangan ini menyebabkannya dapat diretas, dirusak, atau dieksploitasi ketika terjadi serangan DoS (Chithaluru et al., 2021). *Distributed Denial of Service (DDoS)* adalah sebuah serangan yang membuat korban menerima paket masuk terus menerus hingga *trafic* jaringan yang mengarah ke korban mengalami pemakaian bandwidth yang terlalu besar dan mengakibatkan jaringan tersebut tidak berfungsi(Adedeji et al., 2023). Dalam hal ini, DDoS menggunakan sebuah komputer yang berfungsi sebagai master dan bisa mengendalikan komputer yang terinfeksi oleh serangan DoS (slave) dengan melakukan serangan berupa paket yang masuk ke host tujuan sebanyak ribuan atau lebih. Pengiriman paket yang tidak wajar akan mengkibatkan sumber daya server termakan habis dan menyebabkan kinerja server tidak berfungsi sementara bahkan dapat menyebabkan kerusakan permanen pada hardware server tersebut melalui perangkat pribadi atau sumber daya publik, kerugiannya sangat besar(Adedeji et al., 2023; Goud & Giduturi, 2023; Lima Filho et al., 2019). Dengan demikian, permasalahan deteksi anomali trafik di JSN menjadi semakin penting karena trafik anomali dalam jaringan bervariasi, dan serangan serangan DoS di JSN(Putra Pratama & Hari Trisnawan, 2022) (Aighuraibawi et al., 2021; Alexis Fidele et al., 2020; Aljumah, 2017; Gutierrez & Lee, 2020; Majed et al., 2020; Putra Pratama & Hari Trisnawan, 2022)

Pada penelitian ini melakukan perbandingan pola trafik masuk dengan profil trafik asli yang telah ditentukan sebelumnya. Setiap penyimpangan dari profil ini menunjukkan trafik jahat. Profil trafik yang asli diperoleh melalui karakteristik lalu lintas yang terekam ketika terminal yang menghasilkan trafik aman(M. Z. Shafiq et al., 2013) [49]. Salah satu keterbatasan utama pendekatan ini adalah ketidakseimbangan arus lalu lintas karena sifat pola lalu lintas Internet yang dinamis. Hal ini dapat menyebabkan pemilihan fungsi aliran yang salah(Moore & Zuev, 2005). Karena analisis pola trafik memerlukan pola lalu lintas jaringan dikarakterisasi secara akurat untuk akurasi deteksi yang lebih baik, algoritma pembelajaran mesin terutama digunakan. Oleh karena itu, penelitian mengevaluasi potensi pengklasifikasi pembelajaran mesin untuk mengklasifikasikan pola lalu lintas guna meningkatkan deteksi serangan DDoS. Moore dan Zuev mengklasifikasikan pola trafik Internet dengan benar untuk deteksi serangan DDoS menggunakan teknik Bayesian dan memperoleh akurasi 60%. Dalam (Lima Filho et al., 2019), sampel trafik jaringan yang dikumpulkan menggunakan protokol aliran dari perangkat jaringan diklasifikasikan dan dianalisis menggunakan pengklasifikasi False Random (RF). Trafik jaringan dibandingkan dengan tanda tangan yang sebelumnya dikumpulkan dari sampel lalu lintas jaringan untuk melakukan deteksi. Metode ini diuji dengan kumpulan data yang disintesis, terdiri dari kumpulan data CIC-DoS, CICIDS2017 dan CICIDS2018. Berdasarkan hasil, metode tersebut memiliki tingkat deteksi sebesar 96%, tingkat akurasi yang relatif tinggi, dan tingkat alarm palsu. Metode penemuan mempunyai beberapa kelemahan. Membandingkan sampel

Vol 1, No 1, Oktober 2024, Hal 153-162
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

trafik jaringan yang diperoleh sebelumnya. Namun, seiring dengan perubahan beban trafik Internet dari waktu ke waktu, semakin sulit untuk memilih karakteristik aliran yang sesuai, sehingga menyebabkan arus trafik tidak seimbang. Syafiq dll. (M. Shafiq et al., 2018) mengkategorikan fitur trafik menggunakan pendekatan pemilihan fitur berdasarkan pembelajaran mesin hybrid. Dengan menggunakan berbagai data lingkungan jaringan, metode ini mampu memecahkan masalah klasifikasi trafik jarang dalam data tidak seimbang berdimensi tinggi dan mencapai akurasi klasifikasi aliran sebesar 80%. Namun, untuk lalu lintas TCP, hasil sistem tidak terlalu akurat. Beberapa penelusuran tidak hanya mengidentifikasi serangan, namun juga menemukan sumber atau jejaknya.

Metode CUSUM itu mudah proses dan dapat digunakan untuk mendeteksi posisi ubah intinya. Secara khusus, itu telah digunakan uji untuk perubahan mean, varians, dan distribusi fitur(Kim et al., 2004; Xiao et al., 2010). Keuntungan dari metode ini adalah rata-rata sampel, varian, dan distribusi Fungsi dinyatakan sebagai jumlah independen dan variabel acak yang sama memiliki pertimbangkan manfaat sejarah memprediksi seri dan dapat mendeteksi model Ketika kesalahan prediksi adalah Relatif kecil. Algoritma CUSUM dapat dijelaskan dalam empat cara: derivatif yang berbeda. Pertama lebih didasarkan pada intuisi dan menggunakan ide-ide yang terkait dengan ide-ide sederhana Integrasi sinyal dengan ambang adaptif. Bahwa derivasi kedua didasarkan pada online yang lebih formal metode statistik, mirip dengan metode yang digunakan bagan kendali diperkenalkan sebelumnya dan didasarkan pada tentang kemungkinan penggunaan berulang tes rasio. Derivasi ketiga berasal dari menggunakan beberapa tampilan offline hipotetis metode pengujian. Derivasi ini untuk pengantar interpretasi Dengan bantuan algoritma CUSUM V-mask. Bahwa derivasi keempat didasarkan pada konsep pengujian terbuka (Nopiah, Baharin, Abdullah, Khairir dan Nizwan,2008).

Penelitian oleh hanjongkim(Kim et al., 2004) pengembangan metode deteksi perubahan nonparametrik untuk deteksi cepat serangan Denial of Service (DoS) dalam jaringan komputer. Metode yang diusulkan adalah prosedur CUSUM multichart yang menggunakan informasi minimum tentang model lalu lintas sebelum dan sesudah serangan. Penelitian ini menekankan pentingnya respons cepat, tingkat alarm palsu minimal, dan kemampuan untuk mendeteksi berbagai jenis serangan. Hasil simulasi menunjukkan bahwa algoritma CUSUM ini sangat efisien dalam mendeteksi serangan DoS klasik dengan kinerja yang superior dibandingkan metode deteksi lainnya**.** Metode ini juga berhasil menurunkan tingkat alarm palsu yang rendah sebesar **5%**. Serta dalam tindakan mendeteksi serangan dilakukan dengan cepat, dengan detection latency bernilai 2-3 detik. Selain itu hasil dalam penelitian menunjukkan robustness yang baik terhadap variasi lalu lintas dan serangan.

Penelitian oleh (Haydari & Yilmaz, 2018) menunjukkan bahwa dalam mendeteksi dan mitigasi serangan Distributed Denial of Service (DDoS) berbasis RSU pada Sistem Transportasi Intelligent (ITS) dengan menggunakan pendekatan nonparametrik statistik deteksi anomali. Serangan DDoS bertujuan dalam penelitian ini digunakan untuk mengganggu ketersediaan jaringan dengan mengirimkan volume data yang tinggi untuk mengganggu operasi jaringan. Sehingga menjadi permasalah dari segi ketika kecepatan rendah melewati teknik filtering data tradisional akan menjadi sulit dalam mendeteksi deteksi serangan DoS. Kemudia penelitian ini mengusulkan metode nonparametrik yang tidak bergantung pada asumsi distribusi probabilitas, yang menunjukkan kinerja yang lebih baik dalam mendeteksi serangan DDoS dengan kecepatan rendah dibandingkan dengan metode parametrik berbasis Cumulative Sum (CUSUM) dan pendekatan filtering data klasik. Hasil simulasi dalam penelitian ekstensif menggunakan perangkat lunak simulasi trafik SUMO yang menggunakan teknik Generalized CUSUM (G-CUSUM), dan pendekatan filtering data klasik hasilnya delay deteksi rata-rata dan probabilitas false alarm untuk serangan DDoS menyebabkan peningkatan rata-rata yang bernilai 1,5 kali dari data nominal dalam mendeteksi serangan DDoS dengan kecepatan rendah, yang biasanya lebih sulit dideteksi daripada serangan dengan kecepatan tinggi.

Penelitian oleh (H. Liu & Kim, 2010) memperkenalkan jenis serangan DDoS yang disebut "stealthy DDoS attacks," yang dapat diluncurkan oleh penyerang yang canggih. Serangan ini sulit dideteksi dengan metode deteksi Pengenalan Stealthy DDoS mengakibatkan terjadinya peningkatan ambang batas deteksi dengan cara yang lambat dan tersembunyi. Sehingga penelitian ini menggunakan metode deteksi yang berdasarkan dekomposisi waktu-seri yang membagi sederetan FCE menjadi komponen trend dan komponen acak. Kemudian, teknik auto-korelasi ganda dan CUSUM digunakan untuk mendeteksi anomali. Selain itu Metode ini dapat mengurangi tingkat kesalahan positif dan negatif, serta mempercepat waktu deteksi. Selain itu, penggunaan jendela bergerak adaptif membuat metode ini lebih umum digunakan dalam deteksi waktu nyata.hasil penelitian ini menujukkan bahwa Metode yang diusulkan mencapai akurasi deteksi lebih dari 95% dalam mengidentifikasi serangan DDoS yang tersembunyi, jauh mengungguli metode tradisional, Detection Accuracy dari yang terlihat dari rasio positif palsu dikurangi menjadi sekitar 5%, menunjukkan peningkatan substansial dalam membedakan antara lalu lintas normal dan serangan. Dan dari segi Detection Latency menghasilkan nilai yang minimal bernilai 2-3 detik, memungkinkan respons waktu nyata terhadap serangan yang sedang berlangsung. Selain itu hasil Metode ini dapat mempertahankan kinerja tinggi di berbagai pola lalu lintas dan skenario serangan, yang menunjukkan ketahanan dan kemampuan beradaptasinya.

Dalam penelitian ini (Segura et al., 2020) mengembangkan sistem deteksi serangan Denial of Service (DoS) dalam jaringan sensor nirkabel yang terdefinisi oleh perangkat lunak (SDJSN). Sistem ini menggunakan metode deteksi perubahan nonparametrik berbasis CUSUM multichart untuk mendeteksi perubahan mendadak dalam lalu lintas jaringan yang disebabkan oleh serangan DoS. Tujuan penelitian ini dalam menggunakan algoritma ini memiliki kompleksitas komputasi yang dapat dikelola dan optimalitas tertentu, memungkinkan deteksi cepat dengan tingkat alarm palsu yang rendah. Hasil dari simulasi Monte Carlo menunjukkan bahwa metode ini sangat efisien dalam mendeteksi serangan DoS klasik. Selain itu, Menghasilkan tingkat deteksi dan kompleksitas linier yang tinggi dan hasil kinerja detektor penelitian ini pada JSN yang ditentukan perangkat lunak dengan 36 dan 100 node dengan intensitas serangan yang bervariasi (jumlah

Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 153-162
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

penyerang berkisar antara 5% hingga 20% dari node) terjadi peningkat intensitas serangan, pendekatan dalam penelitian ini menghasilkan niliai yang mencapai tingkat deteksi mendekati 100% Dengan demikian, penelitian ini memberikan kontribusi signifikan dalam pengembangan sistem deteksi intrusi yang lebih efektif untuk keamanan jaringan SDJSN. Berdasarkan latar belakang tersebut peneliti bermaksud membuat system pendeteksi DDOS menggunakan algoritma CUSUM (Cummulative Sum) menggunakan data publik dataset DdoS (JSN-DS-New.csv (https://www.kaggle.com/datasets)_ pada Trafik Jaringan Sensor Nirkabel. Sistem ini diharapkan dapat memantau dan mendeteksi jaringan secara proaktif.

2. METODE PENELITIAN

2.1 Kerangka Dasar Penelitian Kerangka Dasar Penelitian

Berdasarkan tahapan penelitian ini dimulai dengan mengindetifikasikan suatu masalah yang berkaitan dengan deteksi serangan DoS, noise, trasmisi yang mempengaruhi kinerja jaringan JSN dan didukung dengan tinjauan Pustaka. Hipotesis dalam penelitian ini diharapkan menghasilkan trafik noise yang bagus dalam memonitoring proses pengiriman dan penerimaan data pada JSN. Selanjutnya menentukan metode penelitian, dimana metode penelitian ini untuk tahap selanjutnya melakukan pemilihan metode yaitu algoritma cusum dan data serangan DoS yang digunakan yaitu dataset JSN-DS khusus untuk yang dikirim (DATA_S) dan data yang diterima (DATA_R), penggunaan energi dan parameter yang digunakan adalah threshold dengan nilai 0,5 sebagai batas yang digunakan untuk mendeteksi serangan atau anomali, nilai weight factor 0,1 sebagai bobot yang diberikan pada observasi baseline dalam algoritma Cusum, dan nilai rata-rata window size 10 sebagai ukuran jendela moving average untuk menghaluskan data, pada tahapan ini juga terdapat processing data, penerapan algoritma cusum, dan analisis noise. Kemudian dilakukan interpretasi untuk mendapatkan hasil deteksi noise dan anomali pada trafik data JSN, dimana proses pengerjaan ini menggunakan MatLab, kemudian penyusunan laporan yang memuat seluruh proses dan tahap akhir selesai, untuk tahapan tersebut dapat dilihat pada Gambar 1.

Gambar 1. Kerangka Dasar Penelitian

2.2 Tahapan Penelitian

Alur dalam penelitian ini langkah awal dimulai dengan Load Dataset DoS attack, kemudian dilanjutkan pemilihan dataset yang mana akan dipilih relevan yang memiliki kolom informasi tentang volume trafik, seperti ukuran paket atau jumlah paket. Setelah memilih kolom trafik, maka dapat menganalisis variable yang digunakan oleh algoritma CUSUM (Putra Pratama & Hari Trisnawan, 2022; Xiao et al., 2010; Ying, 2014) terdiri dari nilai threshold, bobot, dan variable lainnya yang dibutuhkan untuk menghitung CUSUM. Langkah berikutnya adalah menjalankan algoritma CUSUM pada data trafik tang telah diambil dan ini merupakan proses iterative yang memonitor data trafik untuk mendeteksi perubahan yang signifikan (anomali) yang dapat mengindikasikan serangan. Jalan algortima CUSUM terdiri dari dua cabang yaitu deteksi serangan dan analisis dan deteksi data noise. Lalu proses pengujian yang digunakan dalam penelitian ini terdapat 2 proses menggunakan metode algoritma cusum proses pertama pengambilan data kolom, hapus nilai NaN, hitung rata-rata trafik, pada tahapan hitung nilai CUSUM memiliki proses hitung threshold CUSUM, selanjutnya disimpan nilai maksimum CUSUM, jika nilai tersebut adanya terdeteksi serangan maka akan ditampilkan pesan serangan pada monitor, jika tidak terdeteksi serangan maka akan kembali ke hitung nilai CUSUM. Kemudian analisis dan deteksi noisy data. Proses selanjutnya untuk menganalisi dan deteksi data noise dilakukan visualisasi trafik dan nilai CUSUM, hitung moving average, hitung noise, ploy noise data, deteksi noise yang bernilai tinggi, namun jika noise terdeteksi dengan nilai yang tinggi akan diberikan peringatan atau tampilan di monitor, dan jika nilai noise tidak signifikan maka akan lanjut ke tahap analisi berikutnya. Setelah semua Langkah diatas selesai, maka flowchat berakhir, untuk itu dapat dilihat pada Gambar 2. Dalam mendeteksi perubahan kecil yang signifikan dalam data trafik. Teknik algoritma Cusum menghitung perbedaan antara nilai observasi saat ini dan nilai rata-rata (baseline), dan menambahkan hasilnya secara kumulatif untuk mendeteksi perubahan yang terdeteksi. Adapun Persamaan matematika memodifikasi teknik (Putra Pratama & Hari Trisnawan, 2022) yang digunakan dalam penelitian ini sebagai berikut:

a. Persamaan Algoritma Cusum Positif
   Persamaan untuk menghitung cusum Positif pada waktu t :

$$S_t^+ = \max(0, S_{t-1}^+ + (x_t - \mu - T) \quad (1)$$

Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 153-162
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

Keterangan: S^+ digunakan untuk menghitug nilai Cusum positif pada waktu berdasarkan pada nilai waktu cusum positif sebelumnya (S^+_{t-1}), untuk nilai observasi atau data pada waktu t (x_t) dan rata-rata dari baseline (μ) agar mendeteksi perubahan atau anomali yang melebihi threshold yang telah ditentukan (T).

b. Persamaan Cusum Negatif
Cusum negatif untuk mendeteksi penurunan secara tiba-tiba yaitu:

$$S_t^- = \max(0, S_{t-1}^- + (x_t - \mu - T) \quad (2)$$

Keterangan: S_t^- digunakan untuk menghitug nilai Cusum positif pada waktu berdasarkan pada nilai waktu cusum positif sebelumnya (S_{t-1}^-), untuk nilai observasi atau data pada waktu t (x_t) dan rata-rata dari baseline (μ) agar mendeteksi perubahan atau anomali yang melebihi threshold yang telah ditentukan (T).

c. Persamaan Nilai CUSUM (Cumulative Sum)
Persamaan dasar untuk menghitung nilai CUSUM pada langkah waktu t adalah

$$Cusum\ (t,f) = \max(0, Cusum(t-1,f) + .(x(t) - \mu - threshold)) \quad (3)$$

Keterangan : x (t) Nilai trafik yang diamati pada waktu t yang dinilai dari rata-rata trafik (baseline) yang dihitung dari data sebelumnya (μ). Threshold yang digunakan untuk deteksi perubahan (nilai ini ditentukan sebelumnya, dalam kasus ini 0.5 (T). Dengan faktor bobot nilai 0.1yang mengontrol sensitivitas perubahan (w) dalam nilai kumulatif pada waktu t untuk fitur f (Cusum (t,f))

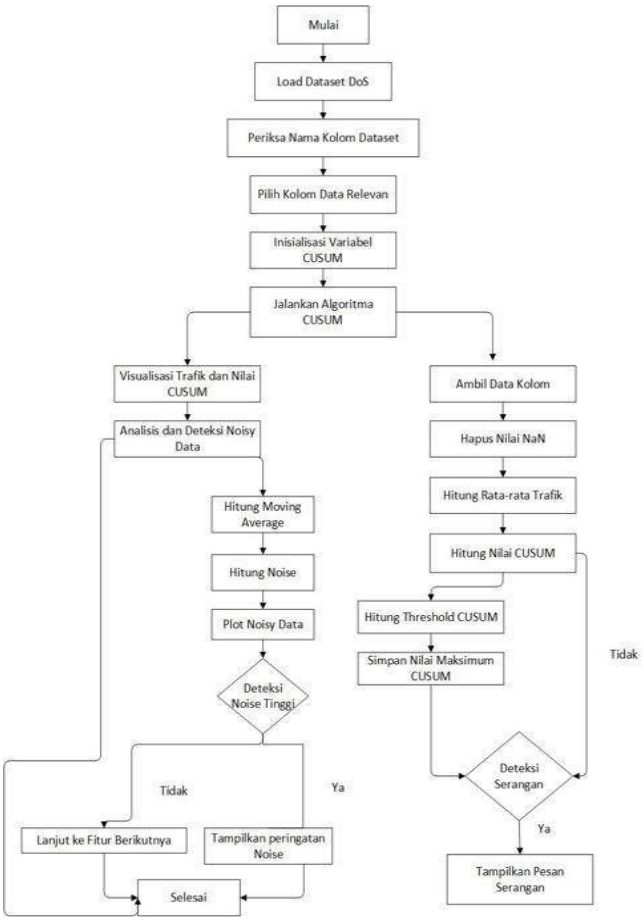
d. Persamaan untuk Threshold Cusum
Cusum juga menghitung ambang batas kumulatif untuk setiap langkah waktu dengan cara yang sama, tetapi mengacu pada nilai data dari waktu sebelumnya, persamaan untuk ambang batas :

$$Cusum\_threshold = \max(0, Cusum\_threshold\ (t,f) + w((x(t-1) - \mu - threshold)) \quad (4)$$

e. Deteksi Serangan
Serangan dideteksi jika nilai cusum melebihi nilai threshold-nya pada langkah waktu t:

$$Attack\_detected\ (t,f)\ jika\ Cusum\ (t,f) > Cusum\_threshold\ (t,f) \quad (5)$$

Keterangan : Jika nilai cusum melebihi ambang batas, kode akan menampilkan pesan bahwa serangan terdeteksi pada waktu tersebut.



Gambar 2. Tahapan Penelitian

Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 153-162
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

3. HASIL DAN PEMBAHASAN

3.1 Pembahasan

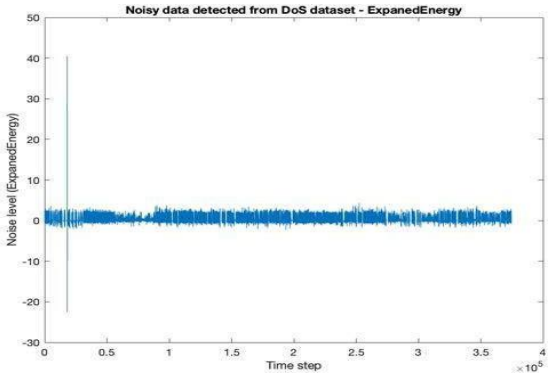
Secara umum, grafik-grafik ini menunjukkan adanya fluktuasi yang sangat besar dalam data, yang berpotensi merupakan hasil dari serangan pada sistem jaringan atau adanya aktivitas abnormal yang menyebabkan peningkatan volume trafik secara tidak wajar. Jika Anda menggunakan algoritma Cusum untuk mendeteksi anomali, maka fluktuasi besar dalam data ini kemungkinan besar terdeteksi sebagai anomali, mengindikasikan adanya serangan atau noise berlebih pada sistem. Hasil Data dari grafik "Noisy data detected from DoS dataset - ExpandedEnergy" tingkat variasi noise yang diukur dari metrik energi dalam konteks serangan Denial of Service (DoS). Grafik ini menghasilkan time step perubahan energi noise dalam sistem pada jaringan dimana pada sumbu X, terdapat adanya time step antara 0 hingga sekitar $4x10^5$, menandakan bahwa dalam pengumpulan data berlangsung dalam periode yang panjang. untuk sumbu Y hasil representasi tingkat noise energi (ExpanedEnergy) terdapat dalam rentang nilai dimulai dari -30 hingga 50. Rentang tersebut menggambarkan nilai variasi fluktuasi energi. Dari hasil grafik tersebut juga terlihat secara keseluruhan adanya pola serangan DoS, yang terdapat adanya lonjakan energi besar pada awal serangan, stabilisasi noise pada sistem, serta terjadinya lonjakan besar dalam tingkat kebisingan energi pada awal pengukuran. Lonjakan yang terjadi pada waktu mendekati nol ini menunjukkan bahwa sistem mengalami peningkatan aktivitas energi yang signifikan akibat gangguan dari luar. Namun, setelah lonjakan awal ini, tingkat noise mulai kembali stabil dan berkisar di sekitar nilai nol, dengan variasi yang relatif kecil. Hal ini menunjukkan bahwa setelah gangguan awal yang mungkin disebabkan oleh serangan, sistem berhasil mencapai kondisi yang lebih stabil. Fluktuasi terdeteksi setelah lonjakan awal yang relatif kecil dan tetap konsisten, mengindikasikan bahwa setelah serangan atau gangguan awal, dampaknya mulai mereda atau sistem mampu menahan efek serangan dengan lebih baik. Lonjakan disebabkan oleh serangan yang menyebabkan peningkatan besar dalam penggunaan sumber daya atau aktivitas sistem. Setelah gangguan awal tersebut, sistem nampak telah berhasil stabil dalam mengurangi tingkat kebisingan, mungkin karena tindakan mitigasi yang diambil atau berkurangnya intensitas serangan, dapat dilihat pada Gambar 3.

Fluktuasi intensitas data yang cukup konsisten di seluruh Time Step untuk *Noisy data* Data S *(Packet Sent*) yang terdeteksi oleh serangan *DoS* berhasil mengumpulkan data dalam time step yang berbeda .Untuk sumbu X menghasilkan Time Step dari 0 hingga sekitar 4 x 10^5 untuk mengumpulkan data. Sedang sumbu Y (tingkat noise DATA_S) menghasilkan kisaran noise antar -200 hingga 200 dalam proses untuk mengumpulkan data. hal ini terjadi karena adanya lonjakan dan munculnya penurunan ketidakstabilan atau noise berulang secara tiba-tiba yang tidak konsisten pada trafik jaringan yang disebabkan oleh serangan DoS. Selain itu, interpretasi tingkat noise tinggi menghasilkan flooding yang mengakibatkan volume paket data berlebihan (tinggi) yang masuk secara mendadak, sehingga pada layanan trafik di jaringan terganggu yang ditunjukkan pada Gambar 4.

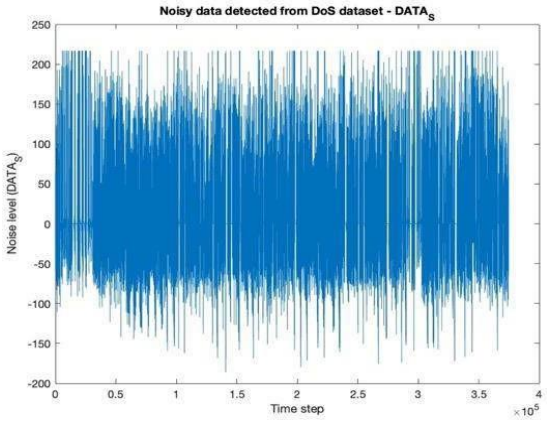
Tampilan hasil kebisingan dengan tingkat kebisingan yang tinggi ketika Noisy dataset Data R (paket data yang diterima) terdeteksi oleh serangan DoS. Hasil grafik sumbu X, data diukur dengan time step menggunakan sampel mencapai 400.000. hasil nilai Ini menunjukkan dataset time series memiliki rentang waktu yang panjan pada jaringan. Untuk grafik sumbu Y menghasil tingkat kebisingan dari dataset rentangnya bernilai dari -1500 hingga 1500. Hasil ini terjadi peningkat kebisingan yang sangat bervariasi secara signifikan dalam nilai data yang fluktuatif di sekitar 0. Fluktuasi intens dan berkelanjutan dalam noise mengindikasikan adanya gangguan atau variasi nilai acak dalam sinyal. Grafik tersebut juga menunjukkan perubahan dalam karakteristik kebisingan selama periode tertentu. Dimana pada tahap awal, nilai antara sekitar 0 hingga 0.5 x 10^5 (50.000) time step untuk tingkat kebisingan relatif lebih rendah dan variasinya lebih kecil. akibanya terjadi lonjakan tajam pada tingkat kebisingan, dan fluktuasi menjadi lebih besar dan lebih sering. Hal ini menandakan terjadinya perubahan signifikan dalam pola kebisingan yang mungkin terhubung dengan kondisi yang berbeda dalam dataset dan terjadinya serangan yang menggangu layanan jaringan atau sistem dalam trafik yang berlebihan. Akibanya terjadinya nilai noise yang tinggi dalam sistem yang abnormal terhadap lonjakan lalu lintas atau serangan paket yang berkelanjutan. Dimana Secara umum, analisis hasil grafik tersebut terjadi lonjakan aktivitas yang fluktuatif, terjadi gangguan atau serangan yang menyebabkan ketidakstabilan sistem. Periode awal hasilnya dataset yang lebih stabil atau dalam kondisi normal sebelum serangan dimulai dan juga terjadi peningkatan drastis pada fase berikutnya mengindikasikan intensitas serangan yang meningkat yang ditunjuk pada Gambar 5.

Nilai pola volume trafik jaringan dari dataset serangan Denial of Service (DoS). Untuk hasil grafik jalur sumbu X, terdapat time step yang mencerminkan pengamatan dari 0 hingga 400.000 unit waktu, sedangkan sumbu Y menunjukkan nilai volume trafik jaringan antara 0 dan 250. Dari grafik ini, terlihat bahwa volume trafik tetap tinggi secara konsisten, akan tetapi ketika nilai 100 hingga 200 unit terjadinya lonjakan data atau permintaan yang signifikan. Dalam Pada awal periode yang berkisar nilai antara 0 hingga 50.000 time step volume trafik yang dilalui terlihat rendah dengan fluktuasi mendekati nol, namun kemudian mengalami peningkatan signifikan yang berlangsung hingga akhir pengamatan. Pola ini sesuai dengan ciri-ciri serangan DoS, di mana penyerang membanjiri jaringan dengan data berlebihan untuk mengganggu kinerja sistem. Meskipun terjadi penurunan volume lalu lintas secara berkala, serangan tersebut secara jelas menimbulkan tekanan besar pada jaringan selama sebagian besar periode pengamatan. Hal ini mengambarkan konsekuensi serangan DoS yang mengakibatkan sistem terbebani, sehingga dapat mengganggu layanan jaringan yang ditunjukkan pada Gambar 6

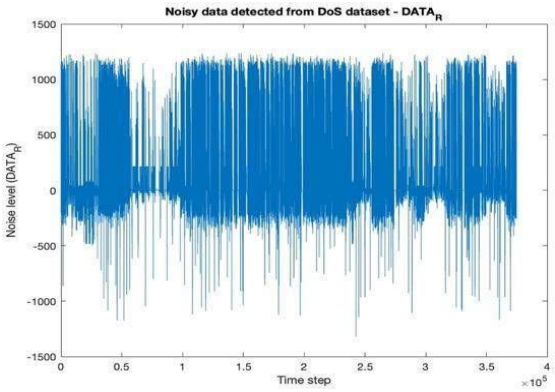
Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 153-162
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad



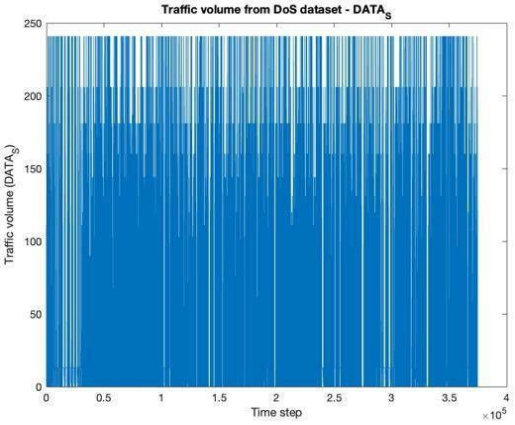
Gambar 1. Noisy dataset-ExpanedEnergy



Gambar 2. Noisy dataset_DataS



Gambar 5. Noisy dataset_DataR



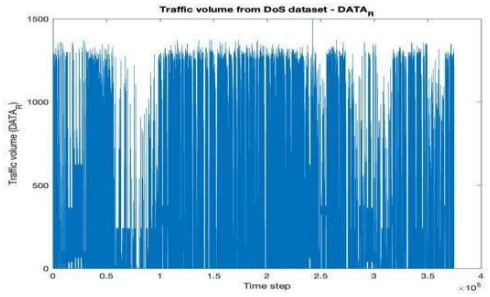
Gambar 6. Traffic dataset_DataS

Volume trafik dari dataset serangan DoS nilai pada fase awal berkisaran time step antar 0 hingga 0.5 x 10^5 relatif

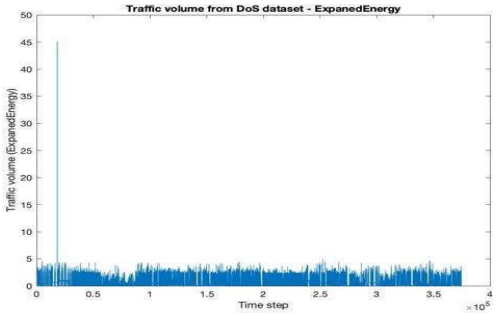
Vol 1, No 1, Oktober 2024, Hal 153-162
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

rendah dan berosilasi sangat signifikan terjadi penurunan nilai volume trafik mendekati nilai 0 yang ditunjukkan pada Gambar 7. Hal ini menunjukkan bahwa terdapat serangan yang belum mencapai titik puncaknya, atau jaringan belum sepenuhnya terbebani oleh serangan. Kemudian Setelah fase awal, yang dimulai dari sekitar nilai 0.5 x 10^5 dalam time step , volume trafik jaringan meningkat secara signifikan hingga mencapai kisaran 1000 hingga 1500 unit, dan keadaan ini berlangsung hingga akhir grafik. Volume trafik tersebut yang konsisten yang bernilai tinggi ini mengindikasikan bahwa jaringan berada di bawah tekanan serangan yang intens, di mana rute trafik data yang sangat besar dikirimkan terus-menerus ke jaringan, yang sesuai dengan karakteristik serangan DoS. Fluktuasi setelah peningkatan terlihat sporadis, dengan penurunan volume lalu lintas yang tiba-tiba. Namun, jumlah penurunan jauh lebih sedikit dibandingkan dengan fase awal. Ini dapat menunjukkan bahwa usaha sistem untuk merespons atau mengurangi dampak serangan, namun secara keseluruhan, serangan terlihat tetap menyebabkan lalu lintas yang tinggi pada jaringan. Dengan pola lalu lintas yang tinggi dan berlangsung lama, grafik menunjukkan potensi overload jaringan dan membanjiri sistem dengan permintaan atau data berlebihan, menyebabkan penurunan kinerja atau kegagalan layanan yang diakibat serangan DoS.

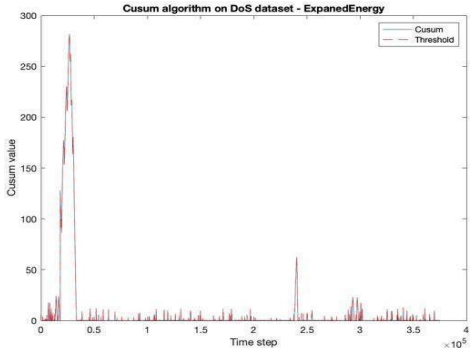
Volume Lalu Lintas dari Dataset DoS - ExpanedEnergy". Hasil pada Sumbu x menghasilkan nilai time step dari 0 hingga sekitar 4 x 10^5, sementara nilai sumbu y menghasilkan volume trafik "ExpandedEnergy", antara dari 0 hingga 50. Hasil tersebut terjadinya adanya nilai lonjakan besar pada volume trafik yang mencapai sekitar 45 unit. Hasil Lonjakan tersebut terjadi karena adanya anomali atau peningkatan trafik data pada awal timeline. Dan untuk hasil Stabilisasi terjadi ketika lonjakan awal, volume trafik yang stabil pada nilai yang lebih rendah antara 0 hingga 5 untuk sisa waktunya. Sehingga konsistensi ada sebagian besar timeline, volume trafik terlihat tetap stabil dengan sedikit fluktuasi, ini menunjukkan adanya serangan yang berkelanjutan atau kondisi trafik stabil setelah anomali awal. Sehingga hasil Grafik trafik selama serangan Denial of Service (DoS), terjadi lonjakan lalu lintas yang besar di awal, yang mungkin dapat membanjiri jaringan, diikuti oleh aktivitas lalu lintas yang lebih rendah namun tetap konstan. Dimana lonjakan awal dapat menandakan dimulainya serangan atau reaksi sistem, sementara tingkat yang lebih rendah menunjukkan lalu lintas berkelanjutan selama fase serangan yang ditunjuk pada Gambar 8.



Gambar 7. Traffic dataset_DataR



Gambar 8. Traffic dataset-ExpanedEnergy

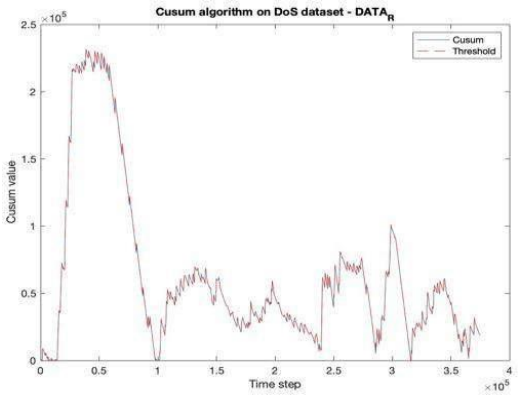


Gambar 9. Cusum dataset-*ExpanedEnergy*

Selanjutnya hasil Grafik pada Gambar 9 ini merupakan tampilan hasil dari penerapan algoritma CUSUM

Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 153-162
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

(Cumulative Sum) pada dataset serangan DoS (Denial of Service) dengan menggunakan variabel "ExpanedEnergy". Dimana teknikAlgoritma CUSUM ini dalam penelitian bertujuan untuk mendeteksi perubahan mendadak atau anomali pada data, yang dalam hal ini, kemungkinan besar terkait dengan serangan DoS berdasarkan pola energi yang dianalisis. Hasil pada nilai sumbu X, mencapai sekitar 4 x 10^5 dalam time step menunjukkan bahwa dataset mencakup ratusan ribu titik waktu. Untuk nilai Sumbu Y menunjukkan nilai CUSUM, yang merupakan total kumulatif dari perubahan energi. Pada hasil Grafik juga menghasilkan dua puncak utama yang mengindikasikan anomali yang signifikan yaitu puncak pertama bernilai antar 0.5 x 10^5 yang artinya hasil ini memilikli lonjakan nilai CUSUM yang sangat tinggi, yang kemungkinan besar mengindikasikan adanya perubahan mendadak yang signifikan, yang diakibatkan oleh serangan DoS. Nilai ini juga mencerminkan aktivitas yang sangat tidak normal di titik awal dataset serta terjadi serangan tiba-tiba yang membanjiri sistem dengan rute trafik jaringan berlebihan. Sedang untuk puncak kedua bernilai antara 2.5 x 10^5 juga menunjukkan anomali, akan tetapi puncaknya jauh lebih kecil dibandingkan dengan puncak pertama. Hal Ini mungkin mencerminkan serangan atau perubahan lain dalam pola energi, meskipun skalanya tidak sebesar anomali awal. Selain itu puncak kedua, memiliki nilai CUSUM relatif rendah dan stabil, terutama setelah titik 3 x 10^5, yang menandakan bahwa tidak ada anomali besar atau perubahan signifikan pada sisa dataset. Selain itu, terdapat garis putus-putus merah yang menunjukkan ambang batas (threshold) untuk deteksi anomali. Jika nilai CUSUM melebihi ambang batas ini, seperti yang terjadi pada dua puncak besar, menunjukkan bahwa perubahan yang terdeteksi dianggap signifikan atau abnormal. Dalam hal ini, baik pada puncak pertama maupun kedua, nilai CUSUM jelas melewati ambang batas, mengonfirmasi adanya aktivitas mencurigakan. Secara keseluruhan, grafik membukti bahwa teknik algoritma CUSUM berhasil mendeteksi dataset secara signifikan. Kemudian Puncak terbesar, yang terjadi di awal, terjadinya serangan DoS utama, yang hasilnya nilai puncak kedua lebih kecil tetapi masih menunjukkan aktivitas anomali. Dan untuk nilai CUSUM yang stabil setelah titik 3 x 10^5 menghasilkan sisa dataset relatif normal tanpa adanya aktivitas serangan yang signifikan.



Gambar 10. Cusum datasey-DataR

Berdasarkan Gambar 10 Grafik ini menunjukkan implementasi algoritma CUSUM pada dataset serangan DoS dengan variabel "DATA_R." (Gambar 10) yang menggunakan teknik Algoritma CUSUM untuk mengidentifikasi perubahan signifikan atau anomali dalam data, khususnya dalam konteks deteksi serangan DoS berdasarkan pola energi atau trafik jaringan. Pada grafik, terdapat puncak pertama sekitar waktu 0.5 x 105, di mana nilai CUSUM meningkat tajam menjadi 2.2 x 105. Puncak ini menunjukkan adanya perubahan kumulatif yang signifikan, yang mungkin menandakan awal dari serangan DoS yang intensif. Serangan ini menyebabkan lonjakan besar pada nilai CUSUM, karena adanya gangguan signifikan dalam pola energi atau trafik tersebut. Setelah puncak ini, nilai CUSUM perlahan menurun pada pola energi yang mulai kembali stabil ketika terjadi serangan pertama. Setelah serangan pertama, antara yang menghasil nilai waktu 1 x 105 hingga 1.5 x 105, merupakan hasil nilai CUSUM yang fluktuasi yang lebih kecil, hal ini menandakan bahwa setelah terjadinya. serangan besar tersebut, hasil pola data menjadi lebih stabil yang artinya dalam pengujian ini tidak ada anomali besar yang terjadi setelahnya, dan aktivitas jaringan atau energi relatif normal selama periode ini. Kemudian, puncak kedua yang bernilai antara waktu 3 x 105, hasil grafik puncak kedua tidak memiliki nilai setinggi puncak pertama, namun tetap menandakan adanya perubahan kumulatif yang signifikan. Puncak kedua ini adanya indikasikan terjadinya serangan DoS yang lebih kecil atau fase lanjutan dari gangguan sebelumnya, namun dengan intensitas yang lebih rendah. Setelah puncak kedua ini, nilai CUSUM menurun, terjadi penurunan anomali bersifat sementara, dan pola energi atau trafik mendekati normal. Setelah waktu antara 3.5 x 105, hasil grafik nilai CUSUM relatif stabil, dengan fluktuasi kecil ini menandakan tidak adanya anomali besar lainnya dalam sisa dataset. Hal ini menunjukkan bahwa setelah kedua puncak besar tersebut, pola energi kembali stabil tanpa adanya perubahan signifikan yang tercatat.

Nilai hasil threshold (ambang batas) yang ditandai digambarkan dengan garis merah putus-putus di grafik menunjukkan batas untuk mendeteksi perubahan yang signifikan. Hasil Nilai CUSUM pada dua puncak utama tersebut melebihi ambang batas, menunjukkan bahwa perubahan tersebut sudah cukup besar untuk dianggap sebagai anomali atau serangan yang signifikan. Penggunaan ambang batas ini penting untuk mengidentifikasi peristiwa signifikan dalam analisis keamanan jaringan. Secara keseluruhan, algoritma CUSUM berhasil menemukan dua anomali besar dalam dataset ini. Puncak pertama besar menunjukkan serangan DoS kuat pada awal dataset. Puncak kedua yang lebih kecil menunjukkan aktivitas mencurigakan yang lebih ringan. Setelah kedua peristiwa tersebut, dataset menunjukkan stabilitas

tanpa adanya anomali besar. Grafik ini menunjukkan pola serangan Denial of Service (DoS), dimulai dengan lonjakan awal yang signifikan dan diikuti oleh stabilisasi setelah serangan menurun.

Pada Gambar 11 merupakan hasil dari penerapan teknik algoritma CUSUM pada dataset serangan DoS (Denial of Service) menggunakan variabel "DATA_S" dalam pengujian untuk mendeteksi perubahan signifikan atau anomali dalam data, terutama terkait dengan aktivitas abnormal oleh serangan DoS. Hasilnya pada fase awal grafik, bernilai antara waktu 0.2 x 10^5, nilai CUSUM tetap mendekati nol, menandakan tidak adanya perubahan atau anomali signifikan yang terdeteksi. Pola ini menunjukkan bahwa aktivitas jaringan berada dalam keadaan normal. Namun, setelah nilai 0.5 x 10^5, nilai CUSUM mulai meningkat perlahan dan stabil, mencapai sekitar 6 x 10^4 pada 2 x 10^5. Kenaikan ini terjadi perubahan kumulatif signifikan yang kemungkinan merupakan tanda awal serangan DoS. Peningkatan nilai CUSUM terjadi karena serangan telah mulai yang mempengaruhi jaringan atau pola energi. Aktivitas serangan atau anomali dalam jaringan mencapai intensitas tertinggi pada titik menghasilkan nilai 2.7 x 10^5 dan nilai CUSUM mencapai puncaknya sekitar 9 x 10^4 nilai CUSUM mulai berfluktuasi secara lebih tajam, dengan naik-turun yang mencerminkan perubahan yang lebih tidak stabil dalam pola data. Fluktuasi ini mungkin mencerminkan fase serangan yang tidak stabil atau gangguan berkala dalam jaringan. Setelah waktu 3 x 10^5, nilai CUSUM mulai menurun secara bertahap, berintensitas serangan atau perubahan kumulatif berkurang, dan jaringan perlahan kembali ke keadaan yang lebih stabil. Di akhir grafik, setelah waktu 3.5 x 10^5, fluktuasi nilai CUSUM menurun, menunjukkan bahwa pola jaringan sudah mendekati kondisi normal.

Garis merah putus-putus pada grafik merupakan ambang batas yang digunakan untuk mendeteksi perubahan signifikan. Pada titik-titik tertentu, seperti pada puncak utama sekitar waktu 2.7 x 10^5, nilai CUSUM melebihi ambang batas, menunjukkan adanya anomali besar yang terdeteksi. Secara keseluruhan, analisis grafik menunjukkan bahwa serangan DoS dimulai setelah waktu 0.5 x 10^5, mencapai puncak utama pada waktu 2.7 x 10^5, kemudian mengalami penurunan intensitas dan stabilisasi jaringan. Algoritma CUSUM mampu mendeteksi perubahan signifikan dengan nilai yang melebihi ambang batas pada titik penting, menunjukkan adanya aktivitas abnormal yang perlu diwaspadai.

4. KESIMPULAN

Berdasarkan hasil pengujian dataset DoS yang dilakukan untuk mengevaluasi nilai traffic, noise, dan teknik CUSUM, dalam deteksi serangan DoS pada Jaringan Sensor Nirkabel dapat dapat disimpulkan algoritma CUSUM mampu mendeteksi serangan DoS dengan tingkat akurasi mendekati 100% baik dalam Dataset data ExpanedEnergy, Dataset DoS ($Data_S$) dan Dataset DoS ($Data_R$). selain itu kesimpulan yang lain dapat dilihat pada tingkat noise untuk Dataset data ExpanedEnergy paling kecil setelah terjadinya lonjakan awal dan cenderung stabil mendekati nol. Sedangkan tingkatan noise yang menggunakan Dataset DoS ($Data_S$) dan Dataset DoS ($Data_R$) memiliki fluktuasi yang besar, dengan Dataset DoS ($Data_R$) yang menunjukkan hasil noise yang paling tidak stabil dan ekstrem. Hal ini terdapat ada anomali atau serangan yang mempengaruhi Dataset DoS ($Data_S$) dan Dataset DoS ($Data_R$), terutama pada fitur Dataset DoS ($Data_R$) yang menunjukkan pola grafik yang terjadi adanya gangguan paling besar oleh serangan DoS. Kemudian volume trafik Dataset DoS ($Data_S$) menghasilkan tingkat volumen yang lebih rendah dengan fluktuasi yang cukup sering, tetapi tidak terlalu ekstrim. Dataset DoS ($Data_R$) menghasilkan pola trafik yang lebih besar dan lebih tidak teratur, dengan lonjakan besar dan penurunan drastis pada interval tertentu. Sehingga dalam hal ini serangan DoS dengan intensitas yang bervariasi, di mana Dataset DoS ($Data_R$) terdeteksi serangan yang lebih agresif atau intens dibandingkan Dataset DoS ($Data_S$).

REFERENCES

Adedeji, K. B., Abu-Mahfouz, A. M., & Kurien, A. M. (2023). DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges. *Journal of Sensor and Actuator Networks*, *12*(4). https://doi.org/10.3390/jsan12040051

Aighuraibawi, A. H. B., Abdullah, R., Manickam, S., & Alyasseri, Z. A. A. (2021). Detection of ICMPv6-based DDoS attacks using anomaly based intrusion detection system: A comprehensive review. *International Journal of Electrical and Computer Engineering*, *11*(6), 5216–5228. https://doi.org/10.11591/ijece.v11i6.pp5216-5228

Alexis Fidele, K., Suryono, & Amien Syafei, W. (2020). Denial of Service (DoS) attack identification and analyse using sniffing technique in the network environment. *E3S Web of Conferences*, *202*. https://doi.org/10.1051/e3sconf/202020215003

Aljumah, A. (2017). Detection of Distributed Denial of Service Attacks Using Artificial Neural Networks. *International Journal of Advanced Computer Science and Applications*, *8*(8), 306–318. https://doi.org/10.14569/ijacsa.2017.080841

Chithaluru, P., Al-Turjman, F., Stephan, T., Kumar, M., & Mostarda, L. (2021). Energy-efficient blockchain implementation for Cognitive Wireless Communication Networks (CWCNs). *Energy Reports*, *7*, 8277–8286. https://doi.org/10.1016/j.egyr.2021.07.136

Goud, K. S., & Gidituri, S. R. (2023). OML-SDN: Detection of DDoS attacks in SDN using Optimized Machine Learning Methods. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(4), 197–208.

Gutierrez, J. N. P., & Lee, K. (2020). An Attack-based Filtering Scheme for Slow Rate Denial-of-Service Attack Detection in Cloud Environment. *Journal of Multimedia Information System*, *7*(2), 125–136. https://doi.org/10.33851/jmis.2020.7.2.125

Haydari, A., & Yilmaz, Y. (2018). Real-Time Detection and Mitigation of DDoS Attacks in Intelligent Transportation Systems. *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC*, *2018-Novem*, 157–163. https://doi.org/10.1109/ITSC.2018.8569698

Kim, H., Rozovskii, B. L., & Tartakovsky, A. G. (2004). A nonparametric multichart CUSUM test for rapid detection of DOS attacks in computer networks. *International Journal of Computing & Information Sciences*, *2*(3), 149–158.

Lima Filho, F. S. De, Silveira, F. A. F., De Medeiros Brito Junior, A., Vargas-Solar, G., & Silveira, L. F. (2019). Smart Detection: An

Online Approach for DoS/DDoS Attack Detection Using Machine Learning. *Security and Communication Networks*, *2019*. https://doi.org/10.1155/2019/1574749

Liu, D., Liang, C., Mo, H., Chen, X., Kong, D., & Chen, P. (2024). LEACH-D: A low-energy, low-delay data transmission method for industrial internet of things wireless sensors. *Internet of Things and Cyber-Physical Systems*, *4*(October 2023), 129–137. https://doi.org/10.1016/j.iotcps.2023.10.001

Liu, H., & Kim, M. S. (2010). Real-time detection of stealthy DDoS attacks using time-series decomposition. *IEEE International Conference on Communications*. https://doi.org/10.1109/ICC.2010.5501975

Majed, H., Noura, H. N., Salman, O., Malli, M., & Chehab, A. (2020). Efficient and secure statistical DDoS detection scheme. *ICETE 2020 - Proceedings of the 17th International Joint Conference on e-Business and Telecommunications*, *Icete*, 153–161. https://doi.org/10.5220/0009873801530161

Mohammed, A., & Misganaw, A. (2022). Modeling future climate change impacts on sorghum (Sorghum bicolor) production with best management options in Amhara Region, Ethiopia. *CABI Agriculture and Bioscience*, *3*(1), 1–17. https://doi.org/10.1186/s43170-022-00092-9

Moore, A. W., & Zuev, D. (2005). *Internet traffic classification using bayesian analysis techniques*. *May*, 50–60. https://doi.org/10.1145/1064212.1064220

Putra Pratama, M., & Hari Trisnawan, P. (2022). Sistem Pendeteksi DDoS menggunakan Algoritma CUSUM pada OpenFlow SDN. *Jurnal Pengembangan Teknologi …*, *6*(5), 2495–2506. http://j-ptiik.ub.ac.id

Segura, G. A. N., Skaperas, S., Chorti, A., Mamatas, L., & Margi, C. B. (2020). Denial of service attacks detection in software-defined wireless sensor networks. *2020 IEEE International Conference on Communications Workshops, ICC Workshops 2020 - Proceedings*. https://doi.org/10.1109/ICCWorkshops49005.2020.9145136

Shafiq, M., Yu, X., Bashir, A. K., Chaudhry, H. N., & Wang, D. (2018). A machine learning approach for feature selection traffic classification using security analysis. *Journal of Supercomputing*, *74*(10), 4867–4892. https://doi.org/10.1007/s11227-018-2263-3

Shafiq, M. Z., Ji, L., Liu, A. X., Pang, J., & Wang, J. (2013). Large-scale measurement and characterization of cellular machine-to-machine traffic. *IEEE/ACM Transactions on Networking*, *21*(6), 1960–1973. https://doi.org/10.1109/TNET.2013.2256431

Xiao, Z., Chen, Z., & Deng, X. (2010). Anomaly detection based on a multi-class CUSUM algorithm for WSN. *Journal of Computers*, *5*(2), 306–313. https://doi.org/10.4304/jcp.5.2.306-313

Ying, B. (2014). CUSUM-based intrusion detection mechanism for wireless sensor networks. *Journal of Electrical and Computer Engineering*, *2014*. https://doi.org/10.1155/2014/245938

Zhao, R., Yin, J., Xue, Z., Gui, G., Adebisi, B., Ohtsuki, T., Gacanin, H., & Sari, H. (2021). An Efficient Intrusion Detection Method Based on Dynamic Autoencoder. *IEEE Wireless Communications Letters*, *10*(8), 1707–1711. https://doi.org/10.1109/LWC.2021.3077946