JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika

[E-ISSN 2656-0321]
[Vol 17 No 2]
[Agustus 2023]

MODEL DETEKSI SERANGAN SSH-BRUTE FORCE BERDASARKAN DEEP BELIEF NETWORK

Constantin menteng [a,1,*], Arief Setyanto[b,2], Hanif Al Fatta[c,3]
[a]Magister Teknik Informatika, Universitas AMIKOM Yogyakarta
[b]Fakultas Sains dan Teknologi, Universitas AMIKOM Yogyakarta
[1]constantin.1283@students.amikom.ac.id, [2]arief_s@amikom.ac.id, [3]hanif@amikom.ac.id
* corresponding author

ARTICLE INFO

Keywords

accuracy
Deep belief network
deep model
F1-score
precession
Restricted Boltzmann Machines
recall

ABSTRACT

Deep Belief Networks are deep learning models that utilize stacks of Restricted Boltzmann Machines (RBM) or sometimes Autoencoders. Autoencoder is a neural network model that has the same input and output. The autoencoder learns the input data and attempts to reconstruct the input data. The solution in this study can provide several tests on DBN such as detecting recall accuracy and better classification precision. By using this algorithm, it is hoped that we as users can overcome problems that occur quite often such as brute force attacks in our accounts and within the company. And the results obtained from this DBN experiment are with an accuracy value of 90.27%, recall 90.27%, precession 91.67%, F1-score 90.51%. The results of this study are the data values of accuracy, recall, precession, and f1-score data used to detect brute force attacks are quite efficient using the deep model of the deep belief network.

1. Pendahuluan

Meningkatnya jumlah ancaman berbahaya pada jaringan komputer dan layanan Internet karena sejumlah besar serangan membuat keamanan jaringan berada pada risiko yang tak henti-hentinya. Keamanan komputer adalah medan pertempuran antara penyerang dan pembela. Metode yang sangat umum digunakan oleh defenders adalah enkripsi. Enkripsi digunakan untuk memastikan bahwa data aman, bahkan jika orang lain mendapatkan data. Akan tetapi, enkripsi yang merupakan pembela memiliki musuh penyerang yang dikenal dengan istilah dekripsi, yang merupakan sebuah cara untuk menyerang pembela yang melindungi data melalui berbagai cara.

Penyerang jaringan komputer telah memperoleh keterampilan tingkat lanjut dan mengeksploitasi kerentanan yang tidak diketahui untuk mem-bypass solusi keamanan. Di antara serangan jaringan terkemuka adalah serangan brute force. Serangan brute force menjadi lebih sulit untuk berhasil dideteksi pada tingkat jaringan karena tumbuh di mana-mana jaringan berkecepatan tinggi dan meningkatkan volume dan enkripsi lalu lintas jaringan. Aplikasi serangan brute force berjalan melalui semua kemungkinan kombinasi karakter legal secara berurutan sampai mereka menemukan input yang benar. Semakin lama kata sandi, semakin banyak waktu yang biasanya diperlukan untuk menemukan input yang benar. Serangan brute force yang paling umum menggunakan kamus kata sandi yang berisi jutaan kata untuk diuji. Serangan brute force yang berhasil tidak hanya memberi peretas akses ke data, aplikasi, dan sumber daya, tetapi juga dapat berfungsi sebagai titik masuk untuk serangan lebih lanjut.[1] Beberapa tanda dapat ditafsirkan sebagai indikator serangan brute force. Diantaranya termasuk, beberapa upaya login yang gagal dari alamat IP yang sama; login dengan beberapa upaya nama pengguna dari alamat IP yang sama; login untuk satu akun dari banyak alamat IP yang berbeda; upaya login yang gagal dari nama pengguna dan kata sandi yang berurutan menurut abjad; login dengan URL perujuk dari email seseorang atau klien IRC.

Secure Shell (SSH) adalah salah satu protokol komunikasi paling populer di Internet yang banyak digunakan oleh pengembang, webmaster, dan administrator sistem. SSH memungkinkan seseorang

https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 17 No 2]
[Agustus 2023]

untuk mendapatkan akses jarak jauh ke layanan cloud baru atau kotak khusus hanya dalam hitungan detik menggunakan saluran komunikasi terenkripsi.[1] Serangan paksa SSH-Brute mencoba untuk mendapatkan akses ke mesin jarak jauh dengan melakukan upaya otentikasi, secara sistematis memeriksa semua kemungkinan kata sandi sampai kata sandi yang benar ditemukan pada protokol Secure Shell. layanan seperti Yahoo atau serangan phishing, mengingat penggunaan kembali kata sandi di seluruh akun tetap merajalela.

Deep Belief Networks merupakan model deep learning yang memanfaatkan tumpukan/stack Restricted Boltzmann Machines (RBM) atau kadangkala Autoencoders. Autoencoder adalah model neural network yang memiliki input dan output yang sama. Autoencoder mempelajari data input dan berusaha untuk melakukan rekonstruksi terhadap data input tersebut. DBN terdiri atas multiple layers dari latent variables (hidden units), dimana masing-masing RBM layer saling terhubung, namun node intra RBM layer tidak saling terhubung dengan node intra RBM layer tidak saling terhubung dengan node intra RBM lainnya.

Maka dari sebab itu metode DBN ini diperlukan untuk melindungi suatu serangan di SSH yang disebabkan dari Brute Force tersebut. Agar tidak terjadi pembobolan kata sandi didalam akun yang dimiliki serta Brute force juga melakukan serangan phishing dalam serangannya.

2. Metodologi Penelitian

2.1. Jenis, sifat, dan pendekatan penelitian

i. Jenis Penelitian

Penelitian ini merupakan penelitian lanjutan dari wanjau, yang mana penelitian itu memiliki data di dalam jurnalnya dan dibandingkan dengan hasil deep learning yaitu Deep Belief Network yang dikerjakan di penelitian ini. Disini bermaksud untuk mengetahui deep model mana yang bagus dalam menganalisa serangan dari brute force.

ii. sifat penelitian

Penelitian ini menjelaskan tahapan-tahapan untuk mengetahui metode yang menghasilkan tingkat akurasi, presisi, recall, dan f1 score yang tinggi dan menganalisis performa suatu model dalam mengklasifikasikan serangan brute force

iii. pendekaatan penelitian kualitatif

Penelitian ini menggunakan pendekatan kuantitatif yaitu hasil dari penerapan metode-metode untuk mengklasifikasikan data berupa angka dan diagram untuk menunjukkan tingkat akurasi dan performa dari penerapan metode-metode tersebut.

2.2. Metode pengumpulan data

Data yang digunakan dalam penelitian ini bersumber dari dataset IDS 2018 intrusion CSVs (CSV-CIC-IDS2018) yang bersumber dari Kaggle. data ini digunakan karena, ini adalah salah satu dari data runjukan dari jurnal internasional sebelumnya yang meneliti dari ISCX IDS 2012. Dan dataset yang digunakan adalah dataset IDS 2018 intrusion CSVs (CSV-CIC-IDS2018) yang didalam dataset tersebut memiliki beberapa serangan dari brute force.

2.3. Metode analisis data

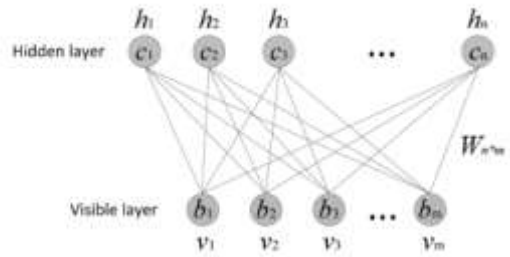
Metode analisis yang digunakan adalah Deep Belief Network (DBN), yang terdiri dari Restricted Boltzman Machine yang melakukan pelatihan layer-wise untuk mencapai eksekusi yang solid dalam

https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 17 No 2]
[Agustus 2023]

domain tanpa pengawasan. Penggunaan RBM yang signifikan kemungkinan akan terjadi, ada kelangkaan data berlabel, dan RBM dan encoder otomatis dapat dilatih sebelumnya pada data yang tidak berlabel dan disesuaikan pada sejumlah kecil data berlabel. Asumsikan sebuah RBM memiliki m sel tersembunyi dan n sel terlihat, vi menunjukkan unit ke-i yang terlihat, hai unit tersembunyi ke-j, dan struktur parameter ditunjukkan seperti pada persamaan.2:

$$W = \{w_{i,j} \in R^{n \times m}\} \tag{2}$$



Gambar 1. arsitektur DBN

di mana wi,j menunjukkan bobot di antara sel terlihat ke-i dan sel tersembunyi ke-j dari persamaan 3.

$$A = \{a_i \in R^{m}\} \tag{3}$$

di mana, ai mewakili ambang bias dari sel yang terlihat ke-i dari persamaan 4;

$$A = \{b_j \in R^{n}\} \tag{4}$$

di mana, bj menunjukkan ambang batas bias sel yang terlihat ke-j. Untuk urutan (v, h) melalui kondisi sekarang, dengan asumsi lapisan tersembunyi dan terlihat mengikuti distribusi Bernoulli, persamaan energi RBM direpresentasikan seperti pada persamaan 5:

$$E(v,h\,|\,\theta) = -\sum_{i=1}^{n} a_i v_i - \sum_{j=1}^{m} b_j h_j - \sum_{i=1}^{n}\sum_{j=1}^{m} v_i W_{ij} h_j \tag{5}$$

dimana, Θ = {Wij, ai, bj} adalah parameter model RBM, dan fungsi energi menunjukkan nilai energi antara estimasi setiap simpul yang terlihat dan setiap lapisan tersembunyi simpul. Karena regularisasi dan eksponensial energi fungsi, persamaan distribusi kemungkinan bersama bisa menjadi diperoleh di mana node mengatur lapisan yang terlihat dan node set lapisan tersembunyi berada dalam kondisi tertentu secara terpisah (v,h) seperti pada persamaan 6:

https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 17 No 2]
[Agustus 2023]

$$P(v,h\,|\,\theta) = \frac{e^{-E(v,h\,|\,\theta)}}{Z(\theta)} \tag{6}$$

$$Z(\theta) = \sum_{v,h} e^{-E(v,h\,|\,\theta)} \tag{7}$$

di mana, dalam persamaan 7, Z(θ) adalah faktor standar atau fungsi distribusi yang menunjukkan eksponen energi total dari setiap kondisi yang tersedia dari himpunan node tersembunyi dan lapisan yang terlihat.

Penentuan fungsi probabilitas sering kali digunakan untuk mendapatkan parameter Setelah mempresentasikan bersama distribusi kemungkinan P(v,h|θ), distribusi marginal P(v|θ) dari kumpulan node dari lapisan yang terlihat dapat diperoleh melalui penjumlahan dari keseluruhan kondisi yang tersembunyi node lapisan diatur dalam persamaan 8:

$$P(v\,|\,\theta) = \frac{1}{Z(\theta)} \sum_{h} e^{-E(v,h\,|\,\theta)} \tag{8}$$

Distribusi marjinal menunjukkan kemungkinan dengan di mana susunan node di lapisan yang terlihat adalah dalam distribusi tingkat tertentu. Karena kecuali- koneksi lapisan-lapisan nasional dan tanpa koneksi antar-lapisan bentuk sistem RBM, ia memiliki signifikansi yang menyertainya kondisi: Setelah mempresentasikan kondisi sel yang terlihat, kondisi berlakunya setiap sel lapisan tersembunyi adalah otonom terbatas. Di sini, kemungkinan inisiasi dari elemen tersembunyi ke-jth adalah seperti yang ditunjukkan pada persamaan 9:

$$P\left(h_j = 1\,|\,v\right) = \sigma(b_j + \sum_i v_i W_{ij}) \tag{9}$$

Dengan demikian, setelah kondisi elemen tersembunyi adalah ditentukan, kemungkinan inisiasi dari elemen yang terlihat tambahan independen bersyarat seperti yang diwakili dalam persamaan 10:

$$P(v_i = 1\,|\,h) = \sigma(a_i + \sum_j W_{ij} h_j) \tag{10}$$

dimana, ô(x) adalah fungsi sigmoid. Untuk memutuskan model RBM, penting untuk menyortir keluarkan tiga parameter model: = {Wij, ai, bj}.Susunan parameter menggunakan probability berfungsi untuk mengambil parameter bawahan. Dari persamaan 8, energi E berbanding terbalik dengan peluang P, dan E terbatas melalui perluasan P. Strategi reguler untuk memperluas masalah fungsional Kemampuan adalah teknik menaikkan kemiringan yang berhubungan dengan perubahan parameter seperti yang ditunjukkan oleh yang menyertai persamaan 11:

https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 17 No 2]
[Agustus 2023]

$$\theta = \theta + \mu \frac{\partial \ln P(v)}{\partial \theta} \quad (11)$$

Proses berulang ini memperluas probabilitas P dan mengurangi energi E.

Aliran algoritma dapat diuraikan sebagai:

Langkah 1: Memulai populasi dan menghasilkan beragam lapisan tersembunyi dan total neuron di setiap lapisan secara acak;

Langkah 2: Hitung tingkat kebugaran sesuai Eq. 1, dipilih oleh teknik roulette, dan pertahankan individu ideal di masa sekarang; interval crossover; variasi;

Langkah 3: "Elite" memegang, memegang individu dengan nilai kebugaran terbaik dalam pengembangan proses;

Langkah 4: Temukan apakah jumlah iterasi tertinggi telah tercapai. Setelah tercapai, struktur jaringan yang dihasilkan adalah held, atau ulangi Step2-Step3 sekali lagi;

Langkah 5: Memanfaatkan struktur jaringan yang optimal untuk DBN dan melatih sistem IDS;

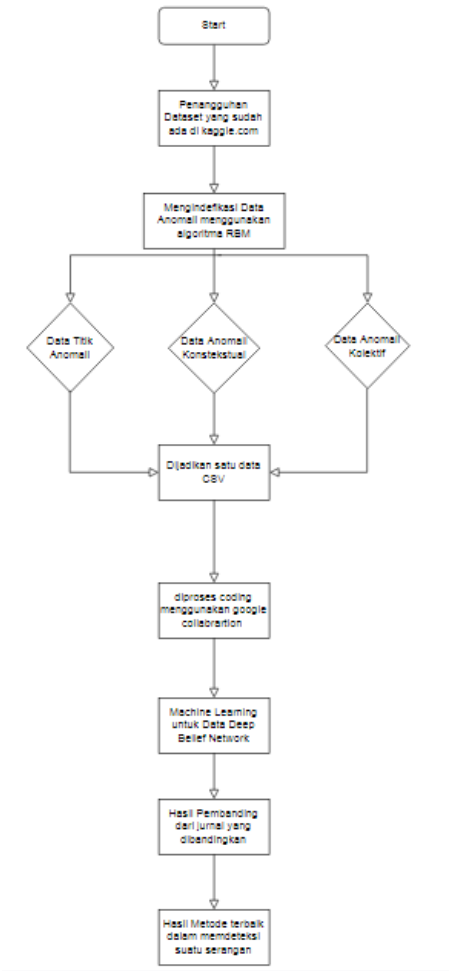
Langkah 6: Mengklasifikasikan set pengujian melalui model DBN terlatih, dan terakhir mengoordinasikan hasil klasifikasi dengan data classification dari set pengujian untuk memvalidasi akurasi klasifikasi.

2.4. Alur penelitian

Alur pertama didalam penelitian adalah mengumpulkan data, lalu ketika sudah terkumpul data-datanya, peneliti mengindentifikasi data-data tersebut menjadi 3 pada data anomali tersebut. Yaitu data titik anomali, data anomali konstektual, dan data anomali kolektif. Ketika ketiga data anomali tersebut selesai di indefikasi lalu semua data tersebut disatukan menjadi CSV (Command Separated Value). Setelah Data CSV tersedia kita inputkan ke dalam machine learning pada DBN untuk mengetahui hasilnya. Setelah mendapatkan hasilnya, dapat dibandingkan dengan hasil data dari peneliti sebelumnya dan memilah dari beberapa algoritma tersebut agar mengetahui hasil yang cukup baik untuk mendeteksinya. Seperti pada gambar * flowchart dibawah ini.

https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 17 No 2]
[Agustus 2023]



Gambar 2. Flowchart

Keterangan :

- Pertama-tama penangguhan dataset dari IDS 2018 intrusion CSVs (CSV-CIC-IDS2018) yang bisa didapatkan dari kaggle.com. didalam dataset tersebut memiliki data-data untuk uji cobanya.
- Mengidentifikasi data anomali dari dataset tersebut menggunakan algoritma RBM
- data anomali terbagi 3 jenis yaitu data titik anomali, data anomali konstektual, dan data anomali kolektif.
- setelah ketiga data di pilah lalu disatukan menjadi satu data CSV
- untuk proses CSVnya menggunakan google collab untuk melakukan uji coba data.
- setelah selesai data tersebut maka akan mendapatkan hasil dari model deep belief network (DBN)
- di bandingkan dengan hasil jurnal sebelumnya yaitu jurnal di [1]
- ketika sudah mendapatkan hasil akurasi yang bagus dari beberapa model tersebut. Dapat dipilah dan di bandingkan hasilnya yang lebih akurat untuk mendeteksi serangan terutama serangan pada brute force.

https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 17 No 2]
[Agustus 2023]

3. Hasil dan Pembahasan

Dalam penelitian ini data yang diteliti adalah deep model yaitu deep belief network dataset yang digunakan adalah IDS 2018 intrusion CSVs (CSV-CIC-IDS2018) di dataset tersebut memiliki berbagai serangan didalamnya, penelitian ini hanya berfokus ke serangan brute force saja.
Didalam dataset tersebut memiliki data 1048576 data terdiri atas benign (jinak) sekitar 665355, setelah itu pada serangan FTP Brute Force 193354 dan SSH- Brute Force memiliki sekitar 187589. Didalam data tersebut akan diambil serangan FTP brute force dan SSH brute force kemudian setelah data telah terkumpul akan di prepocessing ke dalam google colaboratory. Untuk melakukan perkodingan dalam pencarian hasil dari accuracy, precesion, recall, dan F1-score.
Rumus untuk perhitungan DBN :
Accuracy model dievaluasi dalam hal subset dari kinerja model. Akurasi adalah salah satunya pengukuran untuk menilai model klasifikasi data. Dengan perumusan sebagai berikut :

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Presisi menyiratkan tingkat predikatif positif. Ini adalah bagian dari total positif sejati yang dinyatakan model berkorelasi dengan total positif yang dituntutnya. Perumusan presisi sebagai berikut :

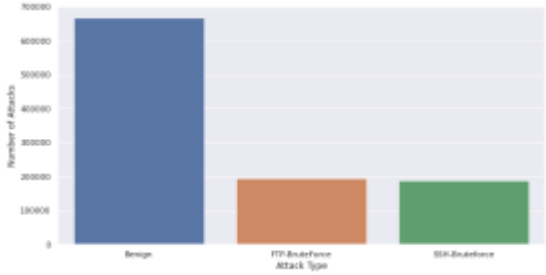
$$Precision = \frac{TP}{TP + FP}$$

Recall dikenal sebagai nilai TP, yang mengacu pada total positif dalam sistem menyatakan kontras dengan total yang tepat positif dalam informasi. Perumusan recall sebagai berikut :

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

F1 score juga dapat digunakan untuk memperkirakan kinerja model. Ini adalah rata-rata tertimbang dari recall dan presisi dari modelnya. Perumusan F1 score sebagai berikut :

$$F1Score = \frac{2 * TP}{2 * TP + FP + FN}$$



Gambar 3. desain dataset

https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 17 No 2]
[Agustus 2023]

Didalam server tersebut memiliki benign (jinak) sekitar 665355, setelah itu pada serangan FTP Brute Force 193354 dan SSH- Brute Force memiliki sekitar 187589.
Tabel Hasil Eksperimen DBN di Google Colaboratory

Tabel 1. Hasil dari penelitian sebelumnya

Kelas	Metrik			
	Accuracy	*Recall*	*Precession*	*F1-Score*
Jinak	0.829	0.883	0.901	0.921
SSH Kasar memaksa	0.852	0.891	0.922	0.894

Tabel 2. Hasil tabel nilai penelitian sekarang

Machine Learning	Metrik			
	Accuracy	*Recall*	*Precession*	*F1- Score*
Deep Belief Network	0.902778	0.9027777777777778	91.67450920770158	0.9051468903110085

Nilai Accuracy pada DBN adalah 0.902778, dan untuk recallnya memiliki nilai angka 0.9027777777777778, nilai dari precession berkisar di angka 91.67450920770158, dan nilai angka terakhir yaitu di F1-score berkisaran diangka 0.9051468903110085. hasil dari nilai tersebut didapatkan di Google Colaborary dan didalam nya tersebut nilainya belum dibuat angka persentase untuk DBN itu sendiri. Jadi untuk mengubah data tersebut untuk menjadi nilai persen peneliti mengambil 4 angka dibelakang koma lalu dikalikan 100% maka akan mendapatkan nilai di accuracy 90,27%, recall 90,27%, precession 91,67%, dan F1-score 90,51%.

4. Kesimpulan

- Dapat disimpulkan dari data yang didapatkan data dari DBN lebih tinggi dari hasil data penelitian sebelumnya. Akan tetapi di precision data yang di dapatkan dari peneliti sebelumnya memiliki nilai lebih tinggi sekitar 0,53% dari data hasil DBN. Deep learning yang diuji didalam ini antara lain adalah CNN k-Nearest Neighbour, Logistic Regression dan Support Vector Machine, dan deep belief network.
- Peneliti dapat berharap agar pada penelitian selanjutnya bisa menggunakan deep learning yang terbaru lagi untuk pencarian datanya. Misalkan seperti Generative Adversial network (GAN)

Daftar Pustaka

[1] S. K. Wanjau, G. M. Wambugu, and G. N. Kamau, "SSH-Brute Force Attack Detection Model based on Deep Learning," *Int. J. Comput. Appl. Technol. Res.*, vol. 10, no. 01, pp. 42–50, 2021, doi: 10.7753/ijcatr1001.1008.

[2] M. Courbariaux, Y. Bengio, and J.-P. David, "Low Precision Storage for Deep Learning," *Iclr*, no. Section 5, p. 10, 2015, [Online]. Available: http://arxiv.org/abs/1511.00363%5Cnhttp://arxiv.org/abs/1412.7024

https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

[3] Z. Munawa and N. I. Putri, "Keamanan IoT Dengan Deep Learning dan Teknologi Big Data," *Temat. J. Teknol. Inf. Komun.*, vol. 7, no. 2, pp. 161–185, 2020, [Online]. Available: https://jurnal.plb.ac.id/index.php/tematik/article/view/479
[4] V. No, S. Sandra, and A. Heryanto, "Visualisasi Serangan Brute Force Menggunakan Metode K-Means dan Naïve Bayes," vol. 2, no. 1, pp. 315–320, 2016.
[5] A. Bimantara, J. S. Komputer, and U. S. Palembang, "Implementasi Machine Learning terhadap Security Management untuk klasifikasi pola traffic TOR pada Intrusion Detection System (IDS)," no. Ml.
[6] A. Zainal, A. Assajjad, S. Si, M. Si, and U. N. Wisesty, "Klasifikasi Sinyal EKG Menggunakan Deep Belief Network dengan Restricted Boltzmann Machine," vol. 5, no. 2, pp. 3623–3630, 2018.
[7] K. R. Kareem Kamoona and C. Budayan, "Implementation of Genetic Algorithm Integrated with the Deep Neural Network for Estimating at Completion Simulation," *Adv. Civ. Eng.*, vol. 2019, 2019, doi: 10.1155/2019/7081073.
[8] T. Aytaç, M. A. Aydın, and A. H. Zaim, "Detection DDOS attacks using machine learning methods," *Electrica*, vol. 20, no. 2, pp. 159–167, 2020, doi: 10.5152/electrica.2020.20049.
[9] S. Priya, "Performance Analysis Comparison on Various Cyber-Attack Dataset By Relating a Deep Belief Network Model on an Intrusion …," *Inf. Technol. Ind.*, vol. 9, no. 3, pp. 608–613, 2021, [Online]. Available: http://www.it-in-industry.org/index.php/itii/article/view/600
[10] K. Highnam, K. Arulkumaran, Z. Hanif, and N. R. Jennings, "BETH Dataset: Real Cybersecurity Data for Unsupervised Anomaly Detection Research," *CEUR Workshop Proc.*, vol. 3095, pp. 1–12, 2021.
[11] M. A. Ferrag, L. Shu, H. Djallel, and K. K. R. Choo, "Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0," *Electron.*, vol. 10, no. 11, pp. 1–26, 2021, doi: 10.3390/electronics10111257.
[12] R. Salakhutdinov and I. Murray, "On the quantitative analysis of deep belief networks," *Proc. 25th Int. Conf. Mach. Learn.*, pp. 872–879, 2008, doi: 10.1145/1390156.1390266.
[13] M. A. Ferrag, L. A. Maglaras, H. Janicke, and R. Smith, "Deep Learning Techniques for Cyber Security Intrusion Detection : A Detailed Analysis," pp. 126–136, 2019, doi: 10.14236/ewic/icscsr19.16.
[14] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective attack detection in internet of medical things smart environment using a deep belief neural network," *IEEE Access*, vol. 8, pp. 77396–77404, 2020, doi: 10.1109/ACCESS.2020.2986013.
[15] A. Z. Agghey, L. J. Mwinuka, S. M. Pandhare, M. A. Dida, and J. D. Ndibwile, "Detection of username enumeration attack on ssh protocol: Machine learning approach," *Symmetry (Basel).*, vol. 13, no. 11, pp. 1–13, 2021, doi: 10.3390/sym13112192.
[16] S. Wali, I. A. Khan, and S. Member, "Explainable AI and Random Forest Based Reliable Intrusion Detection system".
[17] B. C. Merita, "Penerapan Algoritma Restricted Boltzmann Machine Pada Pemilihan Bidang Minat Mahasiswa Informatika Universitas Muhammadiyah Malang," *J. Repos.*, vol. 3, no. 2, pp. 207–214, 2021, doi: 10.22219/repositor.v3i2.1204.
[18] M. I. Mohmand, H. Hussain, A. A. L. I. Khan, and M. Haleem, "A Machine Learning based Classification and Prediction Technique for DDoS Attacks," pp. 1–13, 2017.
[19] M. Scholarworks, "Utilizing Machine Learning Classifiers to Identify SSH Brute Force Attacks Utilizing Machine Learning Classifiers to Identify SSH Brute Force Attacks Advisor : James Deverick," 2019.
[20] I. Odun-ayo, W. Toro-abasi, M. Adebiyi, O. Alagbe, and I. Odun-ayo, "An implementation of real-time detection of cross-site scripting attacks on cloud-based web applications using deep learning," vol. 10, no. 5, pp. 2442–2453, 2021, doi: 10.11591/eei.v10i5.3168.

https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

[E-ISSN 2656-0321]
[Vol 17 No 2]
[Agustus 2023]

[21] Ismail *et al.*, "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," *IEEE Access*, vol. 10, pp. 21443–21454, 2022, doi: 10.1109/ACCESS.2022.3152577.
[22] B. Goparaju and S. R. Bandla, "EasyChair Preprint Distributed Denial of Service Attack Classification Using Artificial Neural Networks .," 2020.

https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI