REDUKSI DIMENSI FITUR SERANGAN *BRUTEFORCE* MENGGUNAKAN METODE *AUTOENCODER LSTM* (AE-LSTM) PADA SISTEM PENDETEKSI SERANGAN SIBER

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH:

RISTI AULIAH UTAMI

09011381924099

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

REDUKSI DIMENSI FITUR SERANGAN *BRUTEFORCE* MENGGUNAKAN METODE *AUTOENCODER LSTM* (AE-LSTM) PADA SISTEM PENDETEKSI SERANGAN SIBER

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH

RISTI AULIAH UTAMI

09011381924099

Indralaya, 27 Juni 2023

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Ir. Sukemi, M. T.	**Ahmad Heryanto,S.Kom.,M.T.**
NIP. 196612032006041001	NIP. 198701222015041002

AUTHENTICATION PAGE

DIMENSIONAL FEATURE REDUCTION OF BRUTEFORCE ATTACKS USING AUTOENCODER LSTM (AE-LSTM) METHOD IN CYBER ATTACK DETECTION SYSTEM

FINAL TASK

Submitted To Fulfill One Of The Requirements

To Obtain A Bachelor's Degree In Computer Science

By

RISTI AULIAH UTAMI

09011381924099

Indralaya, 27 June 2023

Acknowledge,

Head of Computer System Department	***Supervisor***
Ir. Sukemi, M. T.	**Ahmad Heryanto,S.Kom.,M.T.**
NIP. 196612032006041001	NIP. 198701222015041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 25 Mei 2023

Tim Penguji :

1. Ketua Sidang : Ahmad Fali Oklilas, S.T., M.T.
2. Sekretaris Sidang : Abdurahman, S.Kom., M.Han.
3. Penguji Sidang : Iman Saladin B. Azhar, S.Kom., M.MSI.
4. Pembimbing : Ahmad Heryanto, S.Kom., M.T.

Mengetahui, 27/6/23

Ketua Jurusan Sistem Komputer

Ir. Sukemi, M. T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Risti Auliah Utami

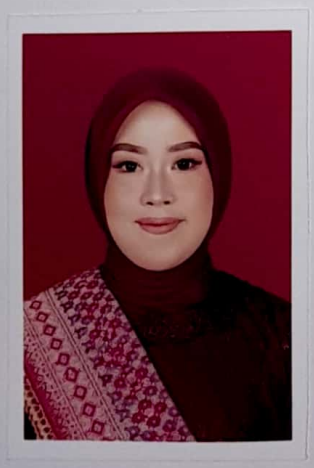
NIM : 09011381924099

Program Studi : Sistem Komputer

Judul : Reduksi Dimensi Fitur Serangan *Bruteforce* Menggunakan Metode *Autoencoder LSTM* (AE-LSTM) pada Sistem Pendeteksi Serangan Siber

Hasil pengecekan *Software IThentivate/Turnitin* : 10%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.



Indralaya, Juni 2023

Penulis,

Risti Auliah Utami

NIM : 09011381924099

HALAMAN PERSEMBAHAN

Terimakasih untuk diriku yang telah berjuang sampai titik ini, hingga kamu berhasil melakukannya! Tapi, perlu diingat bahwa perjuangan belum berhenti sampai di sini. Tetap semangat ya, diriku!

My favorite quote from Al-Qur'an, ***"By the morning brightness, and by the night when it covers with darkness, Your Lord has not taken leave of you, nor has He detested you."*** *(QS. Ad-Dhuha: 1-3).*

This one, for everyone who read this, ***"Setiap orang memiliki sayapnya masing-masing, namun ada beberapa orang yang tak melihat sayap mereka sehingga mereka menjadi takut untuk terbang sama seperti yang lainnya."*** *(Risti A.U).*

"Tugas akhir ini saya persembahkan untuk diri sendiri, orang tua saya, adik-adik saya, teman seperjuangan saya, serta orang-orang yang telah mengambil bagian-bagiannya dalam kehidupan saya, serta orang-orang yang mengajarkan makna serta pengalaman dalam hidup saya. Terimakasih untuk semuanya."

KATA PENGANTAR

Puji dan syukur penulis panjatkan atas kehadirat Allah SWT yang telah melimpahkan rahmat, hidayah, serta karunia-Nya sehingga penulis dapat menyelesaikan penelitian serta penulisan Tugas Akhir yang berjudul "Reduksi Dimensi Fitur Serangan *Bruteforce* Menggunakan Metode *Autoencoder* LSTM (AE-LSTM) pada Sistem Pendeteksi Serangan Siber" .

Penulisan laporan Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Sebagai bahan dalam penulisan, penulis mengambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mendukung dalam penulisan Tugas Akhir ini.

Dalam kesempatan kali ini juga, penulis menyampaikan ucapan terimakasih yang sebesar-besarnya kepada semua pihak yang terlibat serta telah membantu dalam menyelesaikan proses penulisan Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. dan mengucapkan terima kasih kepada yang terhormat :

1. Tuhan Yang Maha Esa Allah SWT. yang telah memberikan rahmat serta karunia-Nya kepada penulis, sehingga penulis dapat menyelesaikan penulisan Tugas Akhir ini,
2. Diri sendiri yang telah berjuang sampai akhir meski menghadapi banyak rintangan serta permasalahan, you got and did it, gurl!
3. Kedua orang tua saya terutama Ibu saya serta adik-adik saya tercinta yang telah memberikan do'a, semangat, serta dukungan kepada saya dalam melaksanakan perkuliahan hingga menyelesaikan Tugas Akhir ini,
4. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya,
5. Bapak Dr. Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya,

6. Bapak Kemahyanto Exaudi,S.Kom.,M.T. selaku Dosen Pembimbing Akademik saya,
7. Bapak Ahmad Heryanto, S.Kom., M.T selaku Dosen pembimbing Tugas Akhir saya, yang telah membimbing dan memberikan kritik, saran serta motivasi terbaik kepada saya dalam mengerjakan dan menyelesaikan Tugas Akhir ini,
8. Kak Agung Al Hafizin sebagai Kakak Tingkat yang telah mengarahkan dan memberikan motivasi kepada saya dalam mengerjakan dan menyelesaikan Tugas Akhir ini,
9. Rianti Agustina dan Wilda Septriyanti selaku sahabat perjuangan yang selalu ada saat dibutuhkan serta yang saya sayangi dan saya banggakan,
10. Teman-teman penghuni Lab.Comnets lantai 2 Kampus Indralaya,
11. Seluruh pihak yang terlibat dalam penulisan Tugas Akhir ini serta seluruh teman-teman angkatan 2019.

Dalam penyusunan Tugas Akhir ini saya selaku penulis menyadari dengan sepenuhnya bahwasanya Tugas Akhir ini masih memiliki kekurangan, oleh karena itu kritik dan saran dari semua pihak yang berkenan agar menjadi bahan evaluasi dan menjadi lebih baik lagi. Akhir kata, saya berharap semoga Tugas Akhir ini dapat bermanfaat serta dapat memberikan pengetahuan dan wawasan bagi semua pihak yang membutuhkannya.

Indralaya, Juni 2023

Penulis,

Risti Auliah Utami

NIM : 09011381924099

REDUKSI DIMENSI FITUR SERANGAN *BRUTEFORCE* MENGGUNAKAN METODE *AUTOENCODER LSTM* (AE-LSTM) PADA SISTEM PENDETEKSI SERANGAN SIBER

Risti Auliah Utami (09011381924099)

Jurusan Sistem Komputer, Fakultas Imu Komputer, Universitas Sriwijaya

Email : ristilitami10@gmail.com

ABSTRAK

Serangan *Bruteforce* merupakan serangan yang menggunakan metode *trial-error* dalam memperoleh informasi pengguna terutama kata sandi. Untuk mengatasi permasalahan tersebut, penelitian terdahulu telah menerapkan algoritma pembelajaran pada sistem pendeteksi serangan siber dan mendapatkan hasil yang memuaskan. Pada pendekatan serangan siber, terdapat kesalahan diagnosis yang bisa timbul akibat data memiliki dimensi yang tinggi. Penelitian ini bertujuan untuk mengaplikasikan algoritma *autoencoder* sebagai metode reduksi dimensi fitur serangan dan algoritma *Long Short-Term Memory* (LSTM) sebagai metode klasifikasi serangan *bruteforce*. Dataset yang digunakan pada penelitian ini adalah dataset CICIDS2018 yang berisi Data Serangan (*FTP-Bruteforce* dan *SSH-Bruteforce*) dan Data Normal (*Benign*). Hasil klasifikasi Data mendapatkan akurasi yang baik yakni sebesar 99.9970%, dengan *Recall* sebesar 99.9970%, *Spesifitas* 99.9969%, *Presisi* 99,9969% dan *F1-Score* sebesar 99.9977%.

Kata Kunci : *Bruteforce, Cyber Attack, Intrusion Detection System (IDS), Autoencoder, LSTM, Dimensionality Reduction, Machine Learning.*

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Ir. Sukemi, M. T.	**Ahmad Heryanto,S.Kom.,M.T.**
NIP. 196612032006041001	NIP. 198701222015041002

DIMENSIONAL FEATURE REDUCTION OF BRUTEFORCE ATTACKS USING AUTOENCODER LSTM (AE-LSTM) METHOD IN CYBER ATTACK DETECTION SYSTEM

Risti Auliah Utami (09011381924099)
Departement of Computer Systems, Faculty of Computer Science, Sriwijaya University
Email : ristilitami10@gmail.com

ABSTRACT

Bruteforce attack is an attack that uses the trial-error method to obtain user information, especially passwords. To overcome these problems, previous research has applied learning algorithms to cyber attack detection systems and obtained satisfactory results. In the cyber attack approach, there is a misdiagnosis that can arise due to high dimensional data. This study aims to apply the autoencoder algorithm as an attack feature dimension reduction method and the Long Short-Term Memory (LSTM) algorithm as a bruteforce attack classification method. The dataset used in this study is the CICIDS2018 dataset which contains Attack Data (FTP-Bruteforce and SSH-Bruteforce) and Normal Data (Benign). Data classification results obtained good accuracy of 99.9970%, with Recall of 99.9970%, Specificity of 99.9969%, Precision of 99.9969% and F1-Score of 99.9977%.

Keywords **:** *Bruteforce, Cyber Attack, Intrusion Detection System (IDS), Autoencoder, LSTM, Dimensionality Reduction, Machine Learning.*

Acknowledge,

Head of Computer System Department	***Supervisor***
Ir. Sukemi, M. T.	**Ahmad Heryanto,S.Kom.,M.T.**
NIP. 196612032006041001	NIP. 198701222015041002

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Cyber security atau keamanan siber yakni seperangkat teknologi atau suatu proses yang telah dirancang untuk melakukan pendeteksian atau pencegahan yang bertujuan untuk melindungi sistem dan jaringan dari akses modifikasi, serta perusakan oleh penyerang [1]. Terdapat banyak metode untuk mendukung keamanan siber ini, contohnya *firewall*, *antivirus*, serta *Instrusion Detection System* (IDS).

Instrusion Detection System (IDS) merupakan suatu metode yang mendukung keamanan siber serta berfungsi untuk mengidentifikasi tindakan kejahatan atau aktivitas yang mecurigakan pada sistem komputer agar keamanan sistem bisa dipertahankan, IDS ini dapat berupa sebuah sistem perangkat lunak maupun perangkat keras. Intrusion Detection System (IDS) ini ditujukkan untuk melakukan identifikasi terhadap *network trafic* yang mencurigakan serta komputer yang tak teridentifikasi oleh firewall yang biasa. Secara luas, metode IDS dapat dibagi menjadi dua, yaitu *Anomaly-based Instrusion Detection System* (AIDS) dan *Signature-based Instrusion Detection System* (SIDS) [2].

Salah satu serangan siber terkemuka yakni serangan *bruteforce*, yang digunakan dalam 89% pelanggaran data atau peretasan berdasarkan laporan dari *Data Breach Investigations Report* 2021 [3]. Serangan *bruteforce* merupakan serangan yang ditujukkan untuk memperoleh informasi pengguna dengan menggunakan metode *trial-error* terutama kata sandi. Penyerang yang menggunakan *bruteforce* terlebih dahulu akan menghimpun segala informasi mendasar dari pengguna [4]. Penyerang tersebut akan terus mencoba kata sandi secara acak berdasarkan informasi pribadi pengguna tersebut dan mengkombinasikan dengan simbol atau karakter lain hingga ditemukan kecocokan. Seiring perkembangan teknologi, penyerang juga membuat alat yang dapat memperoleh kata sandi pengguna secara otomatis [5].

Untuk mengatasi permasalahan akibat serangan *bruteforce,* beberapa penelitian telah menerapkan algoritma pembelajaran pada sistem pendeteksi serangan siber, dalam hal ini adalah *Intrusion Detection System* (IDS) dengan tujuan agar IDS menjadi lebih efisien dan dapat membuat *signature* serangan secara otomatis. Penelitian [6] membahas mengenai berbagai jenis serangan dan anomali pada sistem deteksi intrusi pada IoT, yang dimana terdapat serangan *bruteforce* pada dataset yang digunakan. Penelitian ini mengusulkan model algoritma *Deef Belief Network* (DBN) berbasis *deep learning* pada sistem deteksi instrusi untuk mendeteksi serangan dan anomali dengan dataset yang digunakan adalah CICIDS Dataset 2017 yang dimana serangan pada kumpulan data tersebut terdiri dari serangan *Botnet, DoS/DDoS, Web Attack, infiltration, Bruteforce,* dan *PortScan*. Model yang diusulkan kemudian dibandingkan dengan beberapa model metode deteksi lainnya, dalam hal ini SVM, RNN, SNN dan FNN. Analisis parameter yang digunakan dalam analisis pada penelitian tersebut yakni akurasi, *recall*, presisi, tingkat deteksi, dan *F1-Score*. Model yang diusulkan pada penelitian tersebut mencapai akurasi 97,71% untuk pendeteksian *bruteforce.*

Penelitian [7] membahas mengenai *Intrusion Detection System* (IDS) yang baru berdasarkan dengan algoritma hierarki *Tree-CNN* dengan fungsi aktivasi *Soft-Root-Sign* (SRS). Dalam penelitian ini digunakan tiga dataset, pertama dataset pelatihan dan pengujian model yang diusulkan, dimana dataset tersebut diekstrasi dari kampus universitas dan dua dataset lagi untuk evaluasi kinerja yang diambil dari perusahaan menengah serta CICIDS2017. Serangan-serangan pada dataset dalam peneletian ini terdiri dari *DDoS, Infiltration, Brute Force, dan Web Attack.* Pada penelitian digunakan teknik *Principal Component Analysis* (PCA) sebagai teknik pengurangan dimensi, didapatkan 12 fitur dari 41 fitur yang diekstrasi dari dataset. Setelah mengumpulkan dan mengklasifikasikan data, model yang diusulkan dibandingkan dengan model-model lainnya yakni, *Naïve Bayes, SVM, RF, MLF, Tree-CNN (ReLU) dan Tree-CNN (Softmax)*. Analisis parameter yang digunakan dalam penelitian ini yakni, *Accuracy, Recall, Precision dan F-measure. Model* yang diusulkan mendapatkan hasil yang lebih unggul dibanding dengan model lainnya sebagai pembanding, dengan akurasi mencapai 98% untuk pendeteksian serangan *bruteforce*.

Penelitian-penelitian tersebut menggunakan IDS berbasis anomali atau *Anomaly-based Intrusion Detection System* (AIDS). AIDS merupakan sistem deteksi intrusi yang dibangun dari model matematik atau algoritma sesuai dengan fitur serta label data guna mengukur penyimpangan antara perilaku normal dan serangan. AIDS biasanya menggunakan metode pembelajaran dalam penerapannya. Keuntungan dari metode ini yakni serangan yang baru atau yang tidak diketahui oleh sistem sebelumnya akan dapat segera terdeteksi. Selain memiliki keuntungan, AIDS juga memiliki kekurangan yakni memerlukan data yang ekstensif serta relevan untuk melatih modelnya agar model yang diterapkan dapat secara akurat mendeteksi perilaku menyimpang atau mendeteksi serangan [8]. Dalam penelitian [7] tersebut digunakan metode pengurangan dimensi atau *dimensionality reduction* guna mendapatkan fitur-fitur data yang bersifat relevansi serta informatif yang akan digunakan dalam melatih model mereka.

Dimensionality reduction yakni merupakan sebuah proses yang dilakukan agar dapat menghilangkan fitur yang berlebihan, *noise* pada data, meningkatkan akurasi fitur pembelajaran serta mengurangi waktu training [9]. Definisi lain menyebutkan bahwa reduksi dimensi diperlukan untuk mengurangi dimensi dan mengatasi permasalahan yang timbul akibat data memiliki dimensi yang tinggi, reduksi dimensi juga dapat mengurangi kesalahan diagnosis akibat data yang memiliki dimensi tidak relevan dengan kriteria penelitian serta dapat mengurangi *noise* pada data (*denoising*) [8].

Penelitian [10], [11] dan [12] menerapkan metode *autoencoder* pada tahap reduksi dimensi atau *dimensionality reduction* dan membandingkan hasilnya dengan metode reduksi dimensi tradisional lain. Penelitian yang dilakukan, mendapatkan hasil yang membuktikan bahwa *autoencoder* sebagai metode reduksi dimensi mengungguli metode reduksi dimensi tradisional lainnya, dalam hal ini *Principal Component Analys* (PCA). Mengingat, PCA sebagai metode reduksi dimensi memiliki faktor kelemahan yakni PCA hanya dapat mereduksi data secara linear, sedangkan pada beberapa penelitian terdapat data yang memiliki hubungan secara non-linear.

Dengan berdasarkan uraian-uraian tersebut, penelitian ini akan mengusulkan metode reduksi dimensi fitur serangan *bruteforce* dengan

menggunakan metode *Autoencoder* kemudian hasil dari reduksi dimensi tersebut diklasifikasi menggunakan algoritma *Long Short Term Memory* (LSTM) pada sistem pendeteksi serangan siber.

1.2 Rumusan Masalah

Adapun beberapa rumusan masalah dari latar belakang penelitian serta penulisan tugas akhir ini, dijabarkan sebagai berikut :

1. Bagaimana melakukan tahap reduksi dimensi fitur serangan?
2. Bagaimana menerapkan metode *autoencoder* pada tahap reduksi dimensi fitur untuk proses pendeteksi serangan siber?
3. Bagaimana reduksi dimensi fitur serangan dapat mempengaruhi hasil dari pendeteksian serangan?

1.3 Batasan Masalah

Adapun beberapa batasan masalah dalam penelitian serta penulisan tugas akhir ini yang dijabarkan sebagai berikut :

1. Penelitian ini berfokus pada reduksi dimensi fitur dan klasifikasi serangan *bruteforce* pada dataset IDS dengan algoritma *Autoencoder* dan LSTM.
2. Penelitian ini mengimplementasikan algoritma *Autoencoder* dan LSTM dengan simulasi program python.
3. Penelitian ini akan mempertimbangkan keberhasilan kinerja algoritma *Autoencoder* dan LSTM berdasarkan *confusion matrix*, BACC dan MCC.

1.4 Tujuan

Adapun beberapa tujuan dalam melakukan penelitian serta penulisan tugas akhir ini, yang dijabarkan sebagai berikut :

1. Menerapkan model *Autoencoder* untuk mereduksi dimensi fitur serangan *bruteforce* pada sistem pendeteksi serangan siber berbasis IDS-LSTM.
2. Melakukan pendeteksian terhadap serangan *bruteforce* dengan sistem pendeteksi serangan siber berbasis IDS-LSTM.

3. Memahami serta mengetahui pengaruh dari model *Autoencoder* terhadap efektivitas serta kinerja dari sistem pendeteksi serangan siber berbasis IDS-LSTM.

1.5 Manfaat

Adapun beberapa manfaat yang akan diperoleh dari penelitian serta penulisan tugas akhir ini, yang dijabarkan sebagai berikut :

1. Dapat melakukan reduksi dimensi fitur serangan pada sistem pendeteksi serangan siber dan mempelajari prosesnya.
2. Dapat mengetahui efektivitas serta efisiensi dari menerapkan metode reduksi dimensi dalam pendeteksian serangan.

1.6 Metodelogi Penelitian

Dalam melakukan penelitian serta penulisan tugas akhir ini, terdapat beberapa metode serta tahap yang dilakukan untuk melancarkan proses dalam pengerjaan, sebagai berikut :

1. Metode Perumusan Masalah

   Tahap pertama, penulis melakukan perumusan masalah terkait permasalahan pada pendeteksian serangan siber.
2. Metode Studi Pustaka/Literature

   Tahap kedua, penulis melakukan pencarian dan memahami atau mempelajari referensi terkait pada penelitian ini yang bersumber dari jurnal ilmiah, artikel dan paper lainnya.
3. Metode Konsultasi

   Tahap ketiga, penulis melakukan konsultasi terhadap pihak-pihak yang memiliki wawasan mengenai metode serta model yang diajukan pada penulisan tugas akhir ini.
4. Metode Perancangan dan Pengujian Sistem

   Tahap keempat, penulis akan melakukan perancangan terhadap sistem dengan model yang diajukan pada penulisan tugas akhir ini dan dilakukan pengujian terhadap model telah dibuat tersebut.

5. Metode Analisa dan Kesimpulan

Setelah melakukan serangkaian proses dan mendapatkan hasil dari model yang diajukan, maka akan dilakukan analisa serta membuat kesimpulan dari hasil yang didapatkan.

1.7 Sistematika Penulisan

Untuk penelitian dan penulisan tugas akhir ini, terdapat beberapa sistematika penulisan sebagaimana dijabarkan di bawah ini:

BAB I PENDAHULUAN

Bab pertama ini akan membahas hal-hal yang mendasari penelitian serta penulisan tugas akhir ini, dalam hal ini akan memuat penjabaran dari latar belakang, tujuan dan manfaat, rumusan serta batasan masalah, metodelogi penelitian juga dengan sistematika penulisan dengan pembahasan yang diangkat adalah reduksi dimensi fitur serangan dengan metode *autoencoder* pada sistem deteksi instrusi berbasis LSTM.

BAB II TINJAUAN PUSTAKA

Bab kedua ini akan membahas beberapa tinjauan pustaka beberupa teori pendukung serta literature review terkait dengan reduksi dimensi fitur serangan dengan metode *autoencoder* pada sistem deteksi instrusi berbasis LSTM.

BAB III METODOLOGI PENELITIAN

Bab ketiga ini akan membahas beberapa metodelogi yang akan digunakan pada penelitian tugas akhir ini, dalam hal ini digunakan metode *Autoencoder*-LSTM (AE-LSTM).

BAB IV HASIL DAN ANALISA

Bab keempat ini akan membahas mengenai hasil atau *output* yang didapatkan dari proses penelitian serta dilakukan serta analisa terhadap hasil atau *output* tersebut.

BAB V KESIMPULAN DAN SARAN

Bab terakhir ini akan membahas mengenai kesimpulan serta saran yang diperoleh saat melakukan proses penelitian tugas akhir ini dengan metode atau model yang diajukan.

DAFTAR PUSTAKA

DAFTAR PUSTAKA

[1] M. D. Hossain, H. Ochiai, F. Doudou, and Y. Kadobayashi, "SSH and FTP brute-force attacks detection in computer networks: Lstm and machine learning approaches," *2020 5th Int. Conf. Comput. Commun. Syst. ICCCS 2020*, pp. 491–497, 2020, doi: 10.1109/ICCCS49078.2020.9118459.

[2] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, 2019, doi: 10.1186/s42400-019-0038-7.

[3] E. S. Leet, "About the Cover," *Postmedieval*, vol. 11, no. 1, 2020, doi: 10.1057/s41280-020-00164-x.

[4] K. T. Dave, "Brute-Force Attack 'Seeking but Distressing,'" *Int. J. Innov. Eng. Technol.*, vol. 2, no. 3, pp. 75–77, 2013.

[5] M. M. Najafabadi, T. M. Khoshgoftaar, C. Kemp, N. Seliya, and R. Zuech, "Machine learning for detecting brute force attacks at the network level," *Proc. - IEEE 14th Int. Conf. Bioinforma. Bioeng. BIBE 2014*, pp. 379–385, 2014, doi: 10.1109/BIBE.2014.73.

[6] 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.

[7] R. V. Mendonca *et al.*, "Intrusion Detection System Based on Fast Hierarchical Deep Convolutional Neural Network," *IEEE Access*, vol. 9, pp. 61024–61034, 2021, doi: 10.1109/ACCESS.2021.3074664.

[8] S. Zhao, W. Li, T. Zia, and A. Y. Zomaya, "A dimension reduction model and classifier for anomaly-based intrusion detection in internet of things," *Proc. - 2017 IEEE 15th Int. Conf. Dependable, Auton. Secur. Comput. 2017*

IEEE 15th Int. Conf. Pervasive Intell. Comput. 2017 IEEE 3rd Int. Conf. Big Data Intell. Compu, vol. 2018-Janua, pp. 836–843, 2018, doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.141.

[9] S. Velliangiri, S. Alagumuthukrishnan, and S. I. Thankumar Joseph, "A Review of Dimensionality Reduction Techniques for Efficient Computation," *Procedia Comput. Sci.*, vol. 165, pp. 104–111, 2019, doi: 10.1016/j.procs.2020.01.079.

[10] S. H. A. Shah and S. Rangan, "Multi-cell Multi-beam Prediction using Auto-encoder LSTM for mmWave systems," *IEEE Trans. Wirel. Commun.*, vol. PP, no. Icc, pp. 1–1, 2022, doi: 10.1109/twc.2022.3183632.

[11] M. Yang, D. Zhang, and J. Tao, "Reducing Tongue Shape Dimensionality from Hundreds of Available Resources Using Autoencoder," *Proc. - Int. Conf. Pattern Recognit.*, vol. 2018-Augus, pp. 2875–2880, 2018, doi: 10.1109/ICPR.2018.8545185.

[12] D. C. Ferreira, F. I. Vazquez, and T. Zseby, "Extreme Dimensionality Reduction for Network Attack Visualization with Autoencoders," *Proc. Int. Jt. Conf. Neural Networks*, vol. 2019-July, no. July, pp. 1–10, 2019, doi: 10.1109/IJCNN.2019.8852056.

[13] H. Liu and P. Patras, "NetSentry: A deep learning approach to detecting incipient large-scale network attacks," *Comput. Commun.*, vol. 191, no. October 2021, pp. 119–132, 2022, doi: 10.1016/j.comcom.2022.04.020.

[14] S. S. Volkov and I. I. Kurochkin, "Network attacks classification using Long Short-Term memory based neural networks in Software-Defined Networks," *Procedia Comput. Sci.*, vol. 178, no. 2019, pp. 394–403, 2020, doi: 10.1016/j.procs.2020.11.041.

[15] J. Luxemburk, K. Hynek, and T. Cejka, "Detection of HTTPS Brute-Force Attacks with Packet-Level Feature Set," *2021 IEEE 11th Annu. Comput. Commun. Work. Conf. CCWC 2021*, pp. 114–122, 2021, doi: 10.1109/CCWC51732.2021.9375998.

[16] M. M. Najafabadi, T. M. Khoshgoftaar, C. Calvert, and C. Kemp, “Detection of SSH brute force attacks using aggregated netflow data,” *Proc. - 2015 IEEE 14th Int. Conf. Mach. Learn. Appl. ICMLA 2015*, pp. 283–288, 2016, doi: 10.1109/ICMLA.2015.20.

[17] Y. Yan, L. Qi, J. Wang, Y. Lin, and L. Chen, “A Network Intrusion Detection Method Based on Stacked Autoencoder and LSTM,” *IEEE Int. Conf. Commun.*, vol. 2020-June, 2020, doi: 10.1109/ICC40277.2020.9149384.

[18] S. A. Althubiti, E. M. Jones, and K. Roy, “LSTM for Anomaly-Based Network Intrusion Detection,” *2018 28th Int. Telecommun. Networks Appl. Conf. ITNAC 2018*, pp. 1–3, 2019, doi: 10.1109/ATNAC.2018.8615300.

[19] N. Bakhareva, A. Shukhman, A. Matveev, P. Polezhaev, Y. Ushakov, and L. Legashev, “Attack Detection in Enterprise Networks by Machine Learning Methods,” *Proc. - 2019 Int. Russ. Autom. Conf. RusAutoCon 2019*, no. 16, pp. 1–6, 2019, doi: 10.1109/RUSAUTOCON.2019.8867696.

[20] T. H. Lee, L. H. Chang, and C. W. Syu, “Deep learning enabled intrusion detection and prevention system over SDN networks,” *2020 IEEE Int. Conf. Commun. Work. ICC Work. 2020 - Proc.*, pp. 2–7, 2020, doi: 10.1109/ICCWorkshops49005.2020.9145085.

[21] T. T. H. Le, J. Kim, and H. Kim, “An Effective Intrusion Detection Classifier Using Long Short-Term Memory with Gradient Descent Optimization,” *2017 Int. Conf. Platf. Technol. Serv. PlatCon 2017 - Proc.*, pp. 0–5, 2017, doi: 10.1109/PlatCon.2017.7883684.

[22] B. Eiteneuer, N. Hranisavljevic, and O. Niggemann, “Dimensionality reduction and anomaly detection for cpps data using autoencoder,” *Proc. IEEE Int. Conf. Ind. Technol.*, vol. 2019-Febru, no. 1, pp. 1286–1292, 2019, doi: 10.1109/ICIT.2019.8755116.

[23] Q. Fournier and D. Aloise, “Empirical comparison between autoencoders and traditional dimensionality reduction methods,” *Proc. - IEEE 2nd Int. Conf. Artif. Intell. Knowl. Eng. AIKE 2019*, pp. 211–214, 2019, doi: 10.1109/AIKE.2019.00044.

[24] N. Marir, H. Wang, and G. Feng, “Unsupervised Feature Learning with Distributed Stacked Denoising Sparse Autoencoder for Abnormal Behavior Detection Using Apache Spark,” *Proc. 2nd IEEE Int. Conf. Knowl. Innov. Invent. 2019, ICKII 2019*, pp. 473–476, 2019, doi: 10.1109/ICKII46306.2019.9042645.

[25] B. Abolhasanzadeh, “Nonlinear dimensionality reduction for intrusion detection using auto-encoder bottleneck features,” *2015 7th Conf. Inf. Knowl. Technol. IKT 2015*, 2015, doi: 10.1109/IKT.2015.7288799.

[26] Y. Kanishima, T. Sudo, and H. Yanagihashi, “ScienceDirect ScienceDirect Autoencoder with Adaptive Loss Function Autoencoder with Adaptive Loss Function for Supervised Anomaly Detection for Supervised Anomaly Detection,” *Procedia Comput. Sci.*, vol. 207, pp. 563–572, 2022, doi: 10.1016/j.procs.2022.09.111.

[27] Z. Cheng, E. Zhu, S. Wang, P. Zhang, and W. Li, “Unsupervised Outlier Detection via Transformation Invariant Autoencoder,” *IEEE Access*, vol. 9, pp. 43991–44002, 2021, doi: 10.1109/ACCESS.2021.3065838.

[28] J. Almotiri, K. Elleithy, and A. Elleithy, “Comparison of autoencoder and Principal Component Analysis followed by neural network for e-learning using handwritten recognition,” *2017 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2017*, 2017, doi: 10.1109/LISAT.2017.8001963.

[29] X. Wang and L. Wang, “Research on intrusion detection based on feature extraction of autoencoder and the improved K-means algorithm,” *Proc. - 2017 10th Int. Symp. Comput. Intell. Des. Isc. 2017*, vol. 2, pp. 352–356, 2018, doi: 10.1109/ISCID.2017.170.

[30] R. A. Shaikh and S. V. Shashikala, “An Autoencoder and LSTM based Intrusion Detection approach against Denial of service attacks,” *1st IEEE Int. Conf. Adv. Inf. Technol. ICAIT 2019 - Proc.*, pp. 406–410, 2019, doi: 10.1109/ICAIT47043.2019.8987336.

[31] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A. Beheshti, “Novel Deep Learning-Enabled LSTM Autoencoder Architecture

for Discovering Anomalous Events from Intelligent Transportation Systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4507–4518, 2021, doi: 10.1109/TITS.2020.3017882.

[32] E. Tirado, B. Turpin, C. Beltz, P. Roshon, R. Judge, and K. Gagneja, *A new distributed brute-force password cracking technique*, vol. 878. Springer International Publishing, 2018.

[33] H. C. Chou, H. C. Lee, H. J. Yu, F. P. Lai, K. H. Huang, and C. W. Hsueh, "Password cracking based on learned patterns from disclosed passwords," *Int. J. Innov. Comput. Inf. Control*, vol. 9, no. 2, pp. 821–839, 2013.

[34] T. Gautam and A. Jain, "Analysis of brute force attack using TG-Dataset," *IntelliSys 2015 - Proc. 2015 SAI Intell. Syst. Conf.*, pp. 984–988, 2015, doi: 10.1109/IntelliSys.2015.7361263.

[35] 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.

[36] L. Xia, C. S. Feng, Y. Ding, and W. Can, "Design of secure FTP system," *2010 Int. Conf. Commun. Circuits Syst. ICCCAS 2010 - Proc.*, pp. 270–273, 2010, doi: 10.1109/ICCCAS.2010.5582002.

[37] J. Park, J. Kim, B. B. Gupta, and N. Park, "Network Log-Based SSH Brute-Force Attack DetectionModel," *Comput. Mater. Contin.*, vol. 68, no. 1, pp. 887–901, 2021, doi: 10.32604/cmc.2021.015172.

[38] "Brute Force Attacks: Password Protection." https://www.kaspersky.com/resource-center/definitions/brute-force-attack (accessed Sep. 01, 2022).

[39] "Popular tools for brute-force attacks [updated for 2020] - Infosec Resources." https://resources.infosecinstitute.com/topic/popular-tools-for-brute-force-attacks/ (accessed Sep. 02, 2022).

[40] T. Kakarla, A. Mairaj, and A. Y. Javaid, "A Real-World Password Cracking Demonstration Using Open Source Tools for Instructional Use," *IEEE Int.*

Conf. Electro Inf. Technol., vol. 2018-May, pp. 387–391, 2018, doi: 10.1109/EIT.2018.8500257.

[41] S. Osken, E. N. Yildirim, G. Karatas, and L. Cuhaci, "Intrusion detection systems with deep learning: A systematic mapping study," *2019 Sci. Meet. Electr. Biomed. Eng. Comput. Sci. EBBT 2019*, pp. 1–4, 2019, doi: 10.1109/EBBT.2019.8742081.

[42] U. Bashir and M. Chachoo, "Intrusion detection and prevention system: Challenges & opportunities," *2014 Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2014*, pp. 806–809, 2014, doi: 10.1109/IndiaCom.2014.6828073.

[43] N. T. Van, T. N. Thinh, and L. T. Sach, "An anomaly-based network intrusion detection system using Deep learning," *Proc. - 2017 Int. Conf. Syst. Sci. Eng. ICSSE 2017*, pp. 210–214, 2017, doi: 10.1109/ICSSE.2017.8030867.

[44] A. Phadke, M. Kulkarni, P. Bhawalkar, and R. Bhattad, "A review of machine learning methodologies for network intrusion detection," *Proc. 3rd Int. Conf. Comput. Methodol. Commun. ICCMC 2019*, no. Iccmc, pp. 272–275, 2019, doi: 10.1109/ICCMC.2019.8819748.

[45] D. Selvamani and V. Selvi, "An efficacious intellectual framework for host based intrusion detection system," *Procedia Comput. Sci.*, vol. 165, pp. 9–17, 2019, doi: 10.1016/j.procs.2020.01.014.

[46] M. Chakraborty and M. Singh, "Introduction to Network Security Technologies," *Lect. Notes Networks Syst.*, vol. 163, pp. 3–28, 2021, doi: 10.1007/978-981-15-9317-8_1.

[47] M. Kumar and A. K. Singh, "Distributed Intrusion Detection System using Blockchain and Cloud Computing Infrastructure," *Proc. 4th Int. Conf. Trends Electron. Informatics, ICOEI 2020*, no. Icoei, pp. 248–252, 2020, doi: 10.1109/ICOEI48184.2020.9142954.

[48] "What is an Intrusion Detection System (IDS)? Definition & Types |

Fortinet.” https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system (accessed Sep. 03, 2022).

[49] C. Day, “Intrusion prevention and detection systems,” *Manag. Inf. Secur. Second Ed.*, pp. 119–142, 2013, doi: 10.1016/B978-0-12-416688-2.00005-2.

[50] V. Kanimozhi and T. P. Jacob, “Artificial Intelligence based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing,” *ICT Express*, vol. 5, no. 3, pp. 211–214, 2019, doi: 10.1016/j.icte.2019.03.003.

[51] Q. Zhou and D. Pezaros, “Evaluation of Machine Learning Classifiers for Zero-Day Intrusion Detection -- An Analysis on CIC-AWS-2018 dataset,” no. May 2019, 2019, [Online]. Available: http://arxiv.org/abs/1905.03685.

[52] M. Batta, “Machine Learning Algorithms - A Review,” *Int. J. Sci. Res. (IJ*, vol. 9, no. 1, pp. 381–386, 2020, doi: 10.21275/ART20203995.

[53] M. Aljanabi, M. A. Ismail, and A. H. Ali, “Intrusion detection systems, issues, challenges, and needs,” *Int. J. Comput. Intell. Syst.*, vol. 14, no. 1, pp. 560–571, 2021, doi: 10.2991/ijcis.d.210105.001.

[54] “Supervised vs. Unsupervised Learning: What’s the Difference? | IBM.” https://www.ibm.com/cloud/blog/supervised-vs-unsupervised-learning (accessed Sep. 04, 2022).

[55] H. U. Dike, Y. Zhou, K. K. Deveerasetty, and Q. Wu, “Unsupervised Learning Based On Artificial Neural Network: A Review,” *2018 IEEE Int. Conf. Cyborg Bionic Syst. CBS 2018*, pp. 322–327, 2019, doi: 10.1109/CBS.2018.8612259.

[56] R. Hanocka and H. T. D. Liu, “An introduction to deep learning on meshes,” *ACM SIGGRAPH 2021 Courses, SIGGRAPH 2021*, pp. 1438–1439, 2021, doi: 10.1145/3450508.3464569.

[57] A. Shrestha and A. Mahmood, “Review of deep learning algorithms and architectures,” *IEEE Access*, vol. 7, pp. 53040–53065, 2019, doi:

10.1109/ACCESS.2019.2912200.

[58] X. Du, T. Cai, S. Wang, and L. Zang, “Overivew of Deep Learning,” 2018.

[59] S. Gong, K. Xing, A. Cichocki, and J. Li, “Deep Learning in EEG: Advance of the Last Ten-Year Critical Period,” *IEEE Trans. Cogn. Dev. Syst.*, vol. 14, no. 2, pp. 348–365, 2022, doi: 10.1109/TCDS.2021.3079712.

[60] S. Dong, P. Wang, and K. Abbas, “A survey on deep learning and its applications,” *Comput. Sci. Rev.*, vol. 40, p. 100379, 2021, doi: 10.1016/j.cosrev.2021.100379.

[61] M. Bahi and M. Batouche, “Deep Learning for Ligand-Based Virtual Screening in Drug Discovery,” *Proc. - PAIS 2018 Int. Conf. Pattern Anal. Intell. Syst.*, no. March, 2018, doi: 10.1109/PAIS.2018.8598488.

[62] R. Sadiq, M. J. Rodriguez, and H. R. Mian, *Empirical models to predict disinfection by-products (DBPs) in drinking water: An updated review*, 2nd ed., no. April. Elsevier Inc., 2019.

[63] F. Bre, J. M. Gimenez, and V. D. Fachinotti, “Prediction of wind pressure coefficients on building surfaces using artificial neural networks,” *Energy Build.*, vol. 158, no. November 2017, pp. 1429–1441, 2018, doi: 10.1016/j.enbuild.2017.11.045.

[64] N. M. Rezk, M. Purnaprajna, T. Nordstrom, and Z. Ul-Abdin, “Recurrent Neural Networks: An Embedded Computing Perspective,” *IEEE Access*, vol. 8, pp. 57967–57996, 2020, doi: 10.1109/ACCESS.2020.2982416.

[65] Y. Lu, Y. Shi, G. Jia, and J. Yang, “A new method for semantic consistency verification of aviation radiotelephony communication based on LSTM-RNN,” *Int. Conf. Digit. Signal Process. DSP*, vol. 0, pp. 422–426, 2016, doi: 10.1109/ICDSP.2016.7868592.

[66] M. A. Istiake Sunny, M. M. S. Maswood, and A. G. Alharbi, “Deep Learning-Based Stock Price Prediction Using LSTM and Bi-Directional LSTM Model,” *2nd Nov. Intell. Lead. Emerg. Sci. Conf. NILES 2020*, pp. 87–92, 2020, doi: 10.1109/NILES50944.2020.9257950.

[67] S. Sen and A. Raghunathan, “Approximate Computing for Long Short Term Memory (LSTM) Neural Networks,” *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 37, no. 11, pp. 2266–2276, 2018, doi: 10.1109/TCAD.2018.2858362.

[68] L. Skovajsova, “Long short-term memory description and its application in text processing,” *2017 9th Int. Sci. Conf. Commun. Inf. Technol. KIT 2017 - Proc.*, 2017, doi: 10.23919/KIT.2017.8109465.

[69] W. Wei, H. Wu, and H. Ma, “An autoencoder and LSTM-based traffic flow prediction method,” *Sensors (Switzerland)*, vol. 19, no. 13, pp. 1–16, 2019, doi: 10.3390/s19132946.

[70] “Mengenal 6 Jenis Loss Function pada Machine Learning - Trivusi.” https://www.trivusi.web.id/2022/08/loss-function.html (accessed Oct. 15, 2022).

[71] “Applications | Research | Canadian Institute for Cybersecurity | UNB.” https://www.unb.ca/cic/research/applications.html (accessed Oct. 16, 2022).

[72] V. N. Gudivada, D. Rao, and V. V. Raghavan, *Big Data Driven Natural Language Processing Research and Applications*, vol. 33. Elsevier Inc., 2015.

[73] “Metrics to Evaluate your Machine Learning Algorithm | by Aditya Mishra | Towards Data Science.” https://towardsdatascience.com/metrics-to-evaluate-your-machine-learning-algorithm-f10ba6e38234 (accessed Oct. 16, 2022).

[74] J. Wu, X. Y. Chen, H. Zhang, L. D. Xiong, H. Lei, and S. H. Deng, “Hyperparameter optimization for machine learning models based on Bayesian optimization,” *J. Electron. Sci. Technol.*, vol. 17, no. 1, pp. 26–40, 2019, doi: 10.11989/JEST.1674-862X.80904120.

[75] I. D. Acheme and O. R. Vincent, *Machine-learning models for predicting survivability in COVID-19 patients*. Elsevier Inc., 2021.

[76] N. M. Nawi, W. H. Atomi, and M. Z. Rehman, “The Effect of Data Pre-

processing on Optimized Training of Artificial Neural Networks," *Procedia Technol.*, vol. 11, no. Iceei, pp. 32–39, 2013, doi: 10.1016/j.protcy.2013.12.159.

[77] J. L. Paniagua and J. A. Lopez, "Dimensionality Reduction Applied to Time Response of Linear Systems Using Autoencoders," *2019 IEEE Colomb. Conf. Appl. Comput. Intell. ColCACI 2019 - Proc.*, pp. 1–6, 2019, doi: 10.1109/ColCACI.2019.8781797.

[78] K. El Bouchefry and R. S. de Souza, *Learning in Big Data: Introduction to Machine Learning*. Elsevier Inc., 2020.

[79] Y. Han, Y. Ma, J. Wang, and J. Wang, "Research on ensemble model of anomaly detection based on autoencoder," *Proc. - 2020 IEEE 20th Int. Conf. Softw. Qual. Reliab. Secur. QRS 2020*, pp. 414–417, 2020, doi: 10.1109/QRS51102.2020.00060.

[80] M. Said Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, "Network Anomaly Detection Using LSTM Based Autoencoder," *Q2SWinet 2020 - Proc. 16th ACM Symp. QoS Secur. Wirel. Mob. Networks*, pp. 37–45, 2020, doi: 10.1145/3416013.3426457.

[81] R. Mu and X. Zeng, "A review of deep learning research," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 4, pp. 1738–1764, 2019, doi: 10.3837/tiis.2019.04.001.