OPTIMALISASI ALGORITMA LSTM PADA SISTEM PENDETEKSI SERANGAN BRUTEFORCE MENGGUNAKAN METODE BIDIRECTIONAL LSTM (Bi-LSTM)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

Rianti Agustina

09011181924150

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

HALAMAN PENGESAHAN

OPTIMALISASI ALGORITMA LSTM PADA SISTEM PENDETEKSI SERANGAN BRUTEFORCE MENGGUNAKAN METODE BIDIRECTIONAL LSTM

TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh

Rianti Agustina

09011181924150

Indralaya, 27/6/ Mei 2023

Mengetahui,

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

AUTHENTICATION PAGE

OPTIMIZATION OF THE LSTM ALGORITHM IN A BRUTEFORCE ATTACK DETECTION SYSTEM USING THE BIDIRECTIONAL LSTM (Bi-LSTM) METHOD

FINAL TASK

Submitted To Fulfill One Of The Requirements To Obtain A Bachelor's Degree In Computer Science

By

Rianti Agustina

09011181924150

Indralaya, 29/6/ ~~May~~ 2023

Acknowledge,

Head of Computer System Department	Supervisor
Dr. Ir. H. Sukemi, M.T.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 196612032006041000	**NIP. 198701222015041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Kamis

Tanggal : 25 Mei 2023

Tim Penguji :

1. Ketua : Ahmad Fali Oklilas, M.T

2. Sekretaris : Abdurahman, S.Kom., M.Han

3. Penguji : Iman Saladin B. Azhar, M.MSI

4. Pembimbing : Ahmad Heryanto, S.Kom., M.T

Mengetahui, 29/6/23

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041000

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	: Rianti Agustina
Nim	: 09011181924150
Judul	: Optimalisasi Algoritma LSTM pada Sistem Pendeteksi Serangan Bruteforce Menggunakan Metode Bidirectional LSTM (Bi-LSTM)

Hasil Pengecekan Software Ithenticate/ Turnitin : 6%

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

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Indralaya, Mei 2023

ustina

09011181924150

KATA PENGANTAR

Puji syukur Alhamdulillah penulis panjatkan atas kehadirat Allah SWT yang telah memberikan ridho dan berkah-Nya, sehingga penulis dapat menyelesaikan penyusunan Laporan Tugas Akhir yang berjudul **"Optimalisasi Algoritma LSTM Pada Sistem Pendeteksi Serangan Bruteforce Menggunakan Metode Bidirectional Long Short Term Memory (Bi-LSTM)"**.

Pada Kesempatan ini penulis menyampaikan banyak ucapan terima kasih kepada semua pihak yang telah membantu, memberikan motivasi, kemudahan, pengarahan, bimbingan, dorongan semangat, kritik dan saran selama proses penyusunan Tugas Akhir ini. Oleh karena itu, kesempatan ini penulis bersyukur dan mengucapkan banyak terima kasih kepada:

1. Allah SWT yang telah memberikan saya berkat dan rahmat-Nya serta kesehatan yang berlimpah.
2. Untuk diriku yang sudah berjuang dan melewati masalah-masalah yang sulit.
3. Untuk kedua Orang Tua ku,serta Kakak dan Ayuk yang saya cintai karena telah memberikan motivasi kepada saya.
4. Bapak Jaidan Jauhari, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
6. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing Akademik dan Dosen Pembimbing Skripsi yang telah meluangkan waktunya untuk membimbing serta memberikan saran dan motivasi yang terbaik.
7. Kepada temanku Risti Auliah Utami dan Wilda Septriyanti yang selalu ada dan membantu.
8. Kepada teman-teman kelas SKB 2019 dan teman-teman di lab comnets yang sudah banyak memberikan bantuan.

9. Kakak tingkat Sistem Komputer Universitas Sriwijaya yang selalu memberikan bantuan nya.
10. Dan seluruh pihak yang tidak dapat penulis sebutkan satu per satu, yang selalu memberikan semangat dan bantuan – bantuan yang bermanfaat.

Dalam penulisan laporan Tugas Akhir ini penulis menyadari bahwa pada laporan ini masih banyak kekurangan nya, maka dari itu penulis mengharapkan kritik dan saran dari semua pihak yang berkenan agar menjadi bahan evaluasi dan laporan ini menjadi lebih baik lagi.

Akhir kata penulis ucapkan dan berharap semoga Laporan Tugas Akhir ini dapat bermanfaat serta dapat memberikan pengetahuan dan wawasan bagi semua pihak yang membutuhkannya. Khususnya mahasiswa/i Jurusan Sistem Komputer Universitas Sriwijaya. Saya ucapkan,

Wassalamualaikum Warahmatullahi Wabarakatuh.

Penulis,

Rianti Agustina

NIM.09011181924150

OPTIMALISASI ALGORITMA LSTM PADA SISTEM PENDETEKSI SERANGAN BRUTEFORCE MENGGUNAKAN METODE BIDIRECTIONAL LSTM (Bi-LSTM)

RIANTI AGUSTINA (09011181924150)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : riantiagustina060@gmail.com

ABSTRAK

Serangan bruteforce merupakan bentuk serangan untuk dapat masuk pada layanan jaringan dengan melakukan berbagai pasangan username dan password secara ilegal. Untuk menghindari serangan ini dapat menggunakan karakter yang berbeda-beda kombinasi seperti abjad, alfanumerik, dan alfanumerik dengan simbol. Upaya untuk melindungi sistem keamanan jaringan terhadap serangan Bruteforce, maka dibutuhkan sistem pendeteksi serangan seperti Intrusion Detection System. IDS adalah salah satu pendeteksi yang dapat melakukan penyelidikan terhadap aktivitas yang terjadi pada sistem dan jaringan internet. Metode yang digunakan dalam penelitian ini ialah *Bidirectional Long Short Term Memory* (Bi-LSTM). Pada metode Bi-LSTM terdapat struktur yang berbeda dari LSTM tunggal, dimana Bi-LSTM dapat menghitung data input secara berurutan dan juga urutan terbalik dengan tujuan agar mendapatkan dua status eksternal yang berbeda (dua arah). Selain itu pada metode Bi-LSTM juga memiliki fungsi untuk mengetahui dependensi kontekstual jarak jauh. Penelitian ini menggunakan dua jenis serangan yaitu serangan FTP dan SSH Bruteforce yang diambil dari dataset CIC-IDS 2018. Dengan melakukan validasi pada data training dan testing dari 20% sampai 80%. Sebagai output dari penelitian ini menghasilkan performa nilai yang terbaik berupa Akurasi sebesar 99.9923%, Recall 99.9997%, Spesifitas 99.9815%, Presisi 99.9900%, F1-Score 99.9849%, serta performa nilai dari BACC 99.9906% dan MCC 99.9848%.

Kata kunci : *Serangan Bruteforce, Intrusion Detection Sistem, Dataset CIC-IDS 2018, Bidirectional Long Short Term Memory.*

Mengetahui, 27/6/23

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. H. Sukemi, M.T.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 196612032006041000	**NIP. 198701222015041002**

OPTIMIZATION OF THE LSTM ALGORITHM IN A BRUTEFORCE ATTACK DETECTION SYSTEM USING THE BIDIRECTIONAL LSTM (Bi-LSTM) METHOD

RIANTI AGUSTINA (09011181924150)
Department of Computer Systems, Faculty of Computer Science, Sriwijaya University
Email : riantiagustina060@gmail.com

ABSTRACT

Bruteforce attack is a form of attack to be able to enter network services by making various pairs of usernames and passwords illegally. To avoid this attack you can use different character combinations such as alphabetic, alphanumeric, and alphanumeric with symbols. In an effort to protect network security systems against Bruteforce attacks, an attack detection system such as an Intrusion Detection System is needed. IDS is one of the detectors that can investigate activities that occur on internet systems and networks. The method used in this research is Bidirectional Long Short Term Memory (Bi-LSTM). In the Bi-LSTM method there is a structure that is different from a single LSTM, where Bi-LSTM can calculate input data sequentially and also in reverse order with the aim of obtaining two different external states (two directions). Besides that, the Bi-LSTM method also has a function to find out remote contextual dependencies. This study uses two types of attacks, namely FTP and SSH Bruteforce attacks taken from the CIC-IDS 2018 dataset. By validating training and testing data from 20% to 80%. As the output of this study, the best performance scores were Accuracy of 99.9923%, Recall of 99.9997%, Specificity of 99.9815%, Precision of 99.9900%, F1-Score of 99.9849%, and performance values of BACC of 99.9906% and MCC of 99.9848%.

Keywords : *Bruteforce Attack, Intrusion Detection System, CIC-IDS 2018 Dataset, Bidirectional Long Short Term Memory.*

Acknowledge, 27/6/

Head of Computer System Department	**Supervisor**
Dr. Ir. H. Sukemi, M.T.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 196612032006041000	**NIP. 198701222015041002**

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Balakang

Serangan *bruteforce* adalah bentuk serangan yang dilakukan agar menghasilkan sebuah informasi[1]. Serangan ini bertujuan untuk mencari nama pengguna dan kata sandi secara ilegal dengan mencoba masuk ke beberapa layanan jaringan. Penyerangan *bruteforce* dapat mengeksploitasi keamanan sistem agar bisa memecahkan kata sandi para pengguna. Serangan *bruteforce* sering digunakan peretas karena pada serangan ini mudah untuk diakses yang diambil dari beberapa nama pengguna dan kata sandi. Penyerangan ini dilakukan dengan menggunakan kata sandi dengan fungsi derivasi kunci, yang biasa dikenal dengan pencarian kunci lengkap[2]. Terdapat teknik-teknik yang digunakan untuk mengatasi terjadinya serangan *bruteforce* yaitu dapat memakai password dengan kombinasi yang kompleks, dapat membatasi limit masuk pada password agar terhindar dari serangan, serta melakukan pengamanan website dengan adanya Captcha pada saat memasukkan username dan password.

Terkait penyelidikan dari kecurangan data pada tahun 2020 oleh *Verizon*, diperoleh 80% jumlah pelanggaran yang dilaporkan sebagai data peretasan. Kata sandi yang lemah menjadi salah satu faktor untuk dimanfaatkan peretas dalam melakukan peretasan[3]. Dalam kejadian tersebut, upaya untuk menghindar dari adanya peretas maka kita dapat menerapkan sebuah kata sandi yang rumit. Dimana proses pembuatan kata sandi disarankan untuk set karakter yang berisi huruf kapital, huruf kecil, angka, dan simbol-simbol. Serangan *Bruteforce* biasanya terjadi pada sebuah server, jaringan, atau host dengan mencoba kombinasi password yang sering disebut sebagai “kamus password”. Maka dari itu mekanisme kata sandi dapat menentukan hak akses agar akun terlindungi oleh pihak yang tidak disengaja[4].

Upaya untuk melindungi sistem keamanan jaringan terhadap serangan *Bruteforce*, maka terbentuk teknik-teknik penerapan untuk mencegah terjadinya

serangan tersebut. Terdapat sistem keamanan sebagai pelindung yang telah dibentuk dengan manfaat dan tujuan yang berbeda-beda. Seperti penggunaan *Firewall* difungsikan sebagai pelindung internal terhadap sasaran pada jaringan eksternal. Penggunaan *Virtual Private Network (VPN)* yang fungsinya mengatasi jalur terenkripsi agar aman. Penerapan *Antimalware* yang berguna untuk menghapus sebuah virus yang terdeteksi pada perangkat. Serta penggunaan *Intrusion Detection System (IDS)* salah satu pendeteksi yang dapat melakukan penyelidikan terhadap aktivitas yang terjadi pada setiap sistem dan juga jaringan internet, *IDS* juga berfungsi sebagai mengidentifikasi lalu lintas jaringan tersebut apakah termasuk yang berbahaya atau tidak[2]. Cara kerja dari sistem *IDS* ini dengan mencoba deteksi jaringan lalu lintas yang dipicu oleh alarm, sehingga pada setiap tindakan yang tidak dikenal dapat disebut sebagai serangan yang diakui.

Dalam hal ini *Intrusion Detection System (IDS) dan Long Short Therm Memory (LSTM)* merupakan suatu kombinasi yang tepat dalam menghadapi serangan jaringan salah satunya serangan *Brutefoce*. *LSTM* merupakan hasil modifikasi dari *RNN (Recurrent Neural Network)* yang melengkapi kekurangan dari *RNN*. Sehingga dengan menggunakan *LSTM* sebagai metode dalam penelitian ini dapat memudahkan untuk memprediksi sebuah kata yang berdasarkan dari informasi dahulu yang telah disimpan pada jangka waktu lama, yang mana karena adanya sebuah blok tambahan memory yang disebut *cell*. Pada *LSTM* dapat mengingat informasi dalam jangka waktu panjang dan *LSTM* juga dapat menghapus sebuah informasi yang tidak efektif.

Pada jaringan *LSTM* mampu bekerja dengan baik di berbagai masalah. Untuk menghindari dalam ketergantungan jangka panjang maka *LSTM* dibuat secara eksplisit. Pada dasarnya pencapaian *LSTM* ini sebagai pengingat informasi untuk jangka waktu yang lama[5]. Dengan menggunakan *LSTM* maka dapat secara adaptif dalam mengabaikan masukan tertentu. *LSTM* juga dapat mempertahankan nilai yang dilindungi oleh gerbang yang tidak bisa dilewati dengan fungsi aktivasi[6].

Ada banyak perkembangan dari *LSTM* salah satunya adalah *Bidirectional Long Short Term Memory*. *BiLSTM* merupakan suatu jenis jaringan saraf berulang dan

peningkatan yang melalui jaringan *LSTM*. Terdapat lapisan pada *Bidirectional LSTM* yang fungsinya untuk mengetahui dependensi kontekstual jarak jauh. Keunggulan menggunakan *Bidirectional LSTM* dari *LSTM* tunggal yaitu *Bi-LSTM* dapat menangkap kontekstual informasi dari kedua arah. Pada *Bi-LSTM* terdapat sepasang *LSTM*, dimana *forward LSTM* untuk mengeksekusi sesuai urutan yang dimulai dari kiri ke kanan untuk mengambil konteks masa depan yang akan datang. Dan *backward LSTM* untuk mengeksekusi informasi sesuai urutan dimulai dari kanan ke kiri dengan menangkap konteks sejarah[7]. Struktur dari *Bidirectional LSTM* disini menggunakan dua struktur independen pada jaringan *LSTM*, yang mana jaringan pertama sebagai penghitung data dalam urutan maju dari awal ke akhir urutan dan pada jaringan kedua sebagai penghitung data dalam urutan mundur dari akhir ke awal urutan. Jaringan LSTM forward dan backward akan dimulai dalam keadaan tersembunyi dengan sel yang sama. Dari masing-masing kedua struktur tersebut maka hasil keluarannya akan digabungkan untuk mendapatkan hasil akhir keluaran yang tunggal[8].

Peneliti sebelumnya [9] membahas tentang *pendekatan deep learning untuk IDS menggunakan RNN*, dan mendapatkan nilai *akurasi* sebesar 97.09%. Kemudian peneliti berikutnya [10] *meneliti model LSTM & BiLSTM dalam model pembelajaran hibrid untuk akurasi yang sempurna*, dengan nilai *akurasi* yaitu 93%. Selanjutnya penelitian yang berjudul *serangan jaringan berdasarkan kernel PCA dan LSTM* serta berhasil mendapatkan *akurasi* 98.85%[11]. Dan berdasarkan dari penelitian [13] yang berjudul *RNN dengan menggunakan metode Bidirectional LSTM untuk klasifikasi sentimen* berhasil memperoleh rata-rata *akurasi* sebesar 85.67%.

Berdasarkan uraian-uraian tersebut maka dalam latar belakang yang dibuat oleh penulis akan melakukan penelitian mengenai *Optimalisasi Aloritma LSTM Pada Sistem Pendeteksi Serangan Bruteforce Menggunakan Metode Bidirectional LSTM (Bi-LSTM).* Dimana keunggulan dari metode *Bidirectional LSTM* ini dapat mengekspos beberapa fitur tambahan yang didapatkan. Selain itu, dengan menggunakan *Bidirectional LSTM* dapat membuat hasil output yang diinginkan menjadi maksimal, dikarenakan arsitektur dari *Bidirectional LSTM* ini terdapat dua

lapisan dengan suatu proses yang saling berlawan arah. Maka dari itu, dengan menggunakan *Bidirectional LSTM* akan cocok untuk mengenali pola disetiap kalimat karena dalam metode ini setiap kata nya diproses secara sekuensial.

1.2 Rumusan Masalah

Terdapat beberapa rumusan masalah dalam pelaksaan pada penelitian ini yang akan dibahas sebagai berikut:

1. Bagaimana menerapkan *Bidirectional* LSTM dalam mendeteksi serangan *Bruteforce*?
2. Bagaimana cara kerja *CFS* dalam menghasilkan fitur terbaik untuk deteksi serangan *Bruteforce*?
3. Bagaimanakah hasil dari kemampuan menggunakan metode *Bidirectional* LSTM dalam mendeteksi serangan *Bruteforce* yang berpengaruh pada angka *akurasi*, angka *recall*, angka *spesifitas*, angka *presisi*, angka *F1-Score*, serta angka pada *BACC* dan *MCC*?

1.3 Batasan Masalah

Berikut batasan masalah yang terdapat pada saat melakukan penelitian yaitu seperti di bawah ini:

1. Pada penelitian ini menggunakan jenis serangan *FTP* dan *SSH Bruteforce*
2. Dataset yang dipakai pada penelitian ini yaitu *CIC-IDS 2018*
3. Nilai parameter yang diteliti akan dijadikan sebagai output dari penelitian ini berupa nilai dari *akurasi*, nilai dari *recall*, nilai dari *spesifitas*, nilai *presisi*, nilai *F1-Score*, serta performa nilai dari *BACC* dan performa nilai *MCC*.

1.4 Tujuan Penelitian

Penelitian ini dilakukan berdasar tujuan yang dimiliki agar pelaksaanaan dalam penelitian berjalan lancar, berikut beberapa tujuannya:

1. Untuk menerapkan metode *Bidirectional* LSTM terhadap deteksi serangan Bruteforce
2. Untuk menerapkan *Corelation based Feature Selection* (CFS) sebagai seleksi fitur guna menghasilkan fitur terbaik saat deteksi serangan *Bruteforce.*
3. Untuk menghitung performa hasil kinerja penelitian ini terhadap nilai *akurasi*, nilai *presisi*, nilai *sensitivitas*, nilai *spesifitas*, nilai *F1-Score*, dan nilai *BACC* dan *MCC*.

1.5 Manfaat Penelitian

Di bawah ini merupakan beberapa manfaat yang dapat diambil dari penelitian yaitu sebagai berikut:

1. Bisa memahami cara penerapan algoritma *Bidirectional LSTM* dalam mendeteksi serangan *bruteforce*
2. Dapat memudahkan dalam mengenali serangan bruteforce dengan metode *Bidirectional LSTM*

1.6 Metodologi Penelitian

Di bawah ini terdapat tahap metodologi yang akan dilewati pada saat melakukan penelitian, yaitu sebagai berikut:

1. Metode Studi Literatur

   Pada bagian ini peneliti melakukan pencarian informasi dari berbagai sumber untuk memahami dan mempelajari kajian literatur melalui referensi dari jurnal ilmiah dan beberapa artikel yang berkaitan dengan metode

Bidirectional Long Short Term Memory (Bi-LSTM) sebagai pendukung dalam penelitian.

2. Metode konsultasi

   Pada bagian ini peneliti akan melakukan tanya jawab pada pihak yang terkait yang mempunyai pemahaman dan wawasan yang luas dalam mengatasi terjadinya persoalan terhadap penelitian yang dijalani.

3. Metode Pengumpulan Data

   Dalam tahapan ini peneliti melakukan pengumpulan data yang berhubungan dengan serangan *Bruteforce* serta sistem keamanan *IDS*.

4. Metode Pengujian

   Tahap selanjutnya peneliti akan melatih pengelolaan sistem dan akan diterapkan terhadap penelitian ini guna memperoleh hasil dari mendeteksi serangan *Bruteforce*.

5. Metode Analisa dan Kesimpulan

   Terakhir bagian ini meliputi proses atas keberhasilan yang didapat terhadap pengujian peneliti, yaitu dengan melakukan analisis dari proses pengujian mendeteksi serangan sehingga dapat ditarik sebagai hasil akhir yaitu kesimpulan dalam penelitian ini.

1.7 Sistematika Penulisan

Selanjutnya di bawah ini terdapat penataan penulisan dalam penelitian yaitu seperti berikut:

BAB I PENDAHULUAN

Bagian pertama meliputi bab 1 yaitu penjelasan sistematis berupa pokok penelitian seperti dorongan latar belakang penelitian, tujuan penelitian,

manfaat penelitian, perumusan masalah dalam penelitian, batasan masalah terhadap penelitian, dan metodologi yang digunakan serta yang terakhir mengenai penataan dalam penulisan.

BAB II TINJAUAN PUSTAKA

Pada Bagian bab 2 akan meliputi penjelasan dari dasar teori penelitian mengenai serangan *Bruteforce*, sistem pendeteksi *Intrusion Detection System (IDS)*, dan metode dari *Bidirectional LSTM* yang berkaitan langsung terhadap penelitian ini.

BAB III METODOLOGI PENELITIAN

Kemudian Bab 3 akan membahas metodologi terhadap proses yang dilakukan saat penelitian. Ini akan membuat tahap rancangan sistem deteksi serangan dan menerapkan metodologi yang dibuat untuk penelitian ini.

BAB IV PENGUJIAN DAN ANALISIS

Selanjutnya bab 4 akan meliputi hasil proses dari percobaan yang telah dilaksanakan. Setelah itu melakukan analisa hasil dari data yang didapat saat proses pengujian dengan menggunakan metode *Bidirectional Long Short Term Memory*.

BAB V KESIMPULAN

Dan terakhir untuk bab 5 terdapat beberapa simpulan berdasarkan hasil analisa pada bab sebelumnya dan diperoleh juga saran untuk peneliti selanjutnya sebagai referensi.

DAFTAR PUSTAKA

[1] 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.

[2] J. Zala, A. Panchal, A. Thakkar, B. Prajapati, and P. Puvar, "Intrusion Detection System using Machine Learning," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, no. Icosec, pp. 61–71, 2020, doi: 10.32628/cseit2062166.

[3] TheHackerNews, "Tool Monitoring Baru Free untuk Mengukur Dark Web Exposure," *idNSA*, 2020. https://idnsa.id/article/tool-monitoring-baru-free-untuk-mengukur-dark-web-exposure (accessed Feb. 03, 2023).

[4] L. Li, Q. Zhou, B. Li, and X. Si, "An algorithm to generate password structure dictionary based on gene bank," *Proc. - 2018 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2018*, pp. 11–18, 2019, doi: 10.1109/CyberC.2018.00014.

[5] B. N. Saha and A. Senapati, "Long Short Term Memory (LSTM) based Deep Learning for Sentiment Analysis of English and Spanish Data," *2020 Int. Conf. Comput. Perform. Eval. ComPE 2020*, pp. 442–446, 2020, doi: 10.1109/ComPE49325.2020.9200054.

[6] A. Pulver and S. Lyu, "LSTM with working memory," *Proc. Int. Jt. Conf. Neural Networks*, vol. 2017-May, pp. 845–851, 2017, doi: 10.1109/IJCNN.2017.7965940.

[7] S. Khan *et al.*, "BiCHAT: BiLSTM with deep CNN and hierarchical attention for hate speech detection," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 7, pp. 4335–4344, 2022, doi: 10.1016/j.jksuci.2022.05.006.

[8] S. R. Bin Shah, G. S. Chadha, A. Schwung, and S. X. Ding, "A Sequence-to-Sequence Approach for Remaining Useful Lifetime Estimation Using Attention-

augmented Bidirectional LSTM," *Intell. Syst. with Appl.*, vol. 10–11, p. 200049, 2021, doi: 10.1016/j.iswa.2021.200049.

[9] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[10] M. Kowsher *et al.*, "LSTM-ANN & BiLSTM-ANN: Hybrid deep learning models for enhanced classification accuracy," *Procedia Comput. Sci.*, vol. 193, pp. 131–140, 2021, doi: 10.1016/j.procs.2021.10.013.

[11] F. Meng, Y. Fu, F. Lou, and Z. Chen, "An effective network attack detection method based on kernel PCA and LSTM-RNN," *2017 Int. Conf. Comput. Syst. Electron. Control. ICCSEC 2017*, pp. 568–572, 2018, doi: 10.1109/ICCSEC.2017.8447022.

[12] L. Alawneh, B. Mohsen, M. Al-Zinati, A. Shatnawi, and M. Al-Ayyoub, "A Comparison of Unidirectional and Bidirectional LSTM Networks for Human Activity Recognition," *2020 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2020*, 2020, doi: 10.1109/PerComWorkshops48775.2020.9156264.

[13] A. Aziz Sharfuddin, M. Nafis Tihami, and M. Saiful Islam, "A Deep Recurrent Neural Network with BiLSTM model for Sentiment Classification," *2018 Int. Conf. Bangla Speech Lang. Process. ICBSLP 2018*, pp. 1–4, 2018, doi: 10.1109/ICBSLP.2018.8554396.

[14] 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.

[15] Institute of Electrical and Electronics Engineers, "2020 5th International Conference on Computer and Communication Systems : ICCCS 2020 :

Shanghai, China, May 15-18, 2020.," pp. 138–142, 2020.

[16] J. E. Varghese and B. Muniyal, "An Efficient IDS Framework for DDoS Attacks in SDN Environment," *IEEE Access*, vol. 9, pp. 69680–69699, 2021, doi: 10.1109/ACCESS.2021.3078065.

[17] H. Hou *et al.*, "Hierarchical Long Short-Term Memory Network for Cyberattack Detection," *IEEE Access*, vol. 8, pp. 90907–90913, 2020, doi: 10.1109/ACCESS.2020.2983953.

[18] S. M. Kasongo and Y. Sun, "A deep learning method with filter based feature engineering for wireless intrusion detection system," *IEEE Access*, vol. 7, pp. 38597–38607, 2019, doi: 10.1109/ACCESS.2019.2905633.

[19] S. Naseer *et al.*, "Enhanced network anomaly detection based on deep neural networks," *IEEE Access*, vol. 6, pp. 48231–48246, 2018, doi: 10.1109/ACCESS.2018.2863036.

[20] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection," *2016 Int. Conf. Platf. Technol. Serv. PlatCon 2016 - Proc.*, 2016, doi: 10.1109/PlatCon.2016.7456805.

[21] X. Ma, Z. Dai, Z. He, J. Ma, Y. Wang, and Y. Wang, "Learning traffic as images: A deep convolutional neural network for large-scale transportation network speed prediction," *Sensors (Switzerland)*, vol. 17, no. 4, 2017, doi: 10.3390/s17040818.

[22] C. Li, J. Wang, and X. Ye, "Using a recurrent neural network and restricted boltzmann machines for malicious traffic detection," *NeuroQuantology*, vol. 16, no. 5, pp. 823–831, 2018, doi: 10.14704/nq.2018.16.5.1391.

[23] H. Deng and T. Yang, "Network Intrusion Detection Based on Sparse Autoencoder and IGA-BP Network," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/9510858.

[24] K. Özkan, Ş. Işik, and Y. Kartal, “Evaluation of convolutional neural network features for malware detection,” *6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding*, vol. 2018-Janua, pp. 1–4, 2018, doi: 10.1109/ISDFS.2018.8355390.

[25] S. Nguyen, V. Nguyen, J. Choi, and K. Kim, “Design and Implementation of Intrusion Detection System using Convolutional Neural Network for DoS Detection,” 2018.

[26] M. A. Umar, C. Zhanfang, and Y. Liu, “Network Intrusion Detection Using Wrapper-based Decision Tree for Feature Selection,” *ACM Int. Conf. Proceeding Ser.*, pp. 5–13, 2020, doi: 10.1145/3424311.3424330.

[27] S. Seniaray and R. Jindal, “Machine Learning-Based Network Intrusion Detection System,” *Lect. Notes Data Eng. Commun. Technol.*, vol. 75, pp. 175–187, 2022, doi: 10.1007/978-981-16-3728-5_13.

[28] H. Liu, B. Lang, M. Liu, and H. Yan, “CNN and RNN based payload classification methods for attack detection,” *Knowledge-Based Syst.*, vol. 163, pp. 332–341, 2019, doi: 10.1016/j.knosys.2018.08.036.

[29] A. H. A and K. Sundarakantham, “Machine Learning Based Intrusion,” *2019 3rd Int. Conf. Trends Electron. Informatics*, no. Icoei, pp. 916–920, 2019.

[30] G. Feng, B. Li, M. Yang, and Z. Yan, “V-CNN: Data Visualizing based Convolutional Neural Network,” *2018 IEEE Int. Conf. Signal Process. Commun. Comput. ICSPCC 2018*, 2018, doi: 10.1109/ICSPCC.2018.8567781.

[31] A. Nursetyo, D. R. Ignatius Moses Setiadi, E. H. Rachmawanto, and C. A. Sari, “Website and Network Security Techniques against Brute Force Attacks using Honeypot,” *Proc. 2019 4th Int. Conf. Informatics Comput. ICIC 2019*, 2019, doi: 10.1109/ICIC47613.2019.8985686.

[32] Laatansa, R. Saputra, and B. Noranita, “Analysis of GPGPU-Based Brute-Force and Dictionary Attack on SHA-1 Password Hash,” *ICICOS 2019 - 3rd Int. Conf.*

Informatics Comput. Sci. Accel. Informatics Comput. Res. Smarter Soc. Era Ind. 4.0, Proc., pp. 1–4, 2019, doi: 10.1109/ICICoS48119.2019.8982390.

[33] A. Borkar, A. Donode, and A. Kumari, "A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)," *Proc. Int. Conf. Inven. Comput. Informatics, ICICI 2017*, no. Icici, pp. 949–953, 2018, doi: 10.1109/ICICI.2017.8365277.

[34] M. Aguk and N. Anggraini, "Uji Fitur Intrusion Prevention Pada Firewall Untangle Dengan Pengujian Dos Dan Ssh Brute Force," *J. Manaj. Inform.*, vol. 9, pp. 18–25, 2018.

[35] L. Yang, J. Li, G. Fehringer, P. Barraclough, and G. Sexton, "Intrusion Detection System by Fuzzy Interpolation," 2017.

[36] A. A. Aburomman and M. B. I. Reaz, "Survey of learning methods in intrusion detection systems," *2016 Int. Conf. Adv. Electr. Electron. Syst. Eng. ICAEES 2016*, no. Ml, pp. 362–365, 2017, doi: 10.1109/ICAEES.2016.7888070.

[37] S. Das and M. J. Nene, "A survey on types of machine learning techniques in intrusion prevention systems," *Proc. 2017 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2017*, vol. 2018-Janua, pp. 2296–2299, 2018, doi: 10.1109/WiSPNET.2017.8300169.

[38] S. Ray, "A Quick Review of Machine Learning Algorithms," *Proc. Int. Conf. Mach. Learn. Big Data, Cloud Parallel Comput. Trends, Prespectives Prospect. Com. 2019*, pp. 35–39, 2019, doi: 10.1109/COMITCon.2019.8862451.

[39] M. P. Hosseini, A. Hosseini, and K. Ahi, "A Review on Machine Learning for EEG Signal Processing in Bioengineering," *IEEE Rev. Biomed. Eng.*, vol. 14, no. c, pp. 204–218, 2021, doi: 10.1109/RBME.2020.2969915.

[40] S. Loussaief and A. Abdelkrim, "Machine Learning framework for image classification," *Adv. Sci. Technol. Eng. Syst.*, vol. 3, no. 1, pp. 1–10, 2018, doi: 10.25046/aj030101.

[41] H. Hu, M. Liao, C. Zhang, and Y. Jing, “Text classification based recurrent neural network,” *Proc. 2020 IEEE 5th Inf. Technol. Mechatronics Eng. Conf. ITOEC 2020*, no. Itoec, pp. 652–655, 2020, doi: 10.1109/ITOEC49072.2020.9141747.

[42] T. Liu, T. Wu, M. Wang, M. Fu, J. Kang, and H. Zhang, “Recurrent Neural Networks based on LSTM for Predicting Geomagnetic Field,” *ICARES 2018 - Proc. 2018 IEEE Int. Conf. Aerosp. Electron. Remote Sens. Technol.*, vol. 5, pp. 56–60, 2018, doi: 10.1109/ICARES.2018.8547087.

[43] X. Xu, H. Ge, and S. Li, “An improvement on recurrent neural network by combining convolution neural network and a simple initialization of the weights,” *Proc. 2016 IEEE Int. Conf. Online Anal. Comput. Sci. ICOACS 2016*, pp. 150–154, 2016, doi: 10.1109/ICOACS.2016.7563068.

[44] J. Xu, R. Rahmatizadeh, L. Boloni, and D. Turgut, “A Sequence Learning Model with Recurrent Neural Networks for Taxi Demand Prediction,” *Proc. - Conf. Local Comput. Networks, LCN*, vol. 2017-Octob, pp. 261–268, 2017, doi: 10.1109/LCN.2017.31.

[45] P. Sahithya, M. Arulmozhi, and N. Praveen, “Digital design of radial basis function neural network and recurrent neural network,” *2019 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2019*, pp. 393–397, 2019, doi: 10.1109/WiSPNET45539.2019.9032759.

[46] L. Burgueño, J. Cabot, and S. Gérard, “An LSTM-Based Neural Network Architecture for Model Transformations,” *Proc. - 2019 ACM/IEEE 22nd Int. Conf. Model Driven Eng. Lang. Syst. Model. 2019*, pp. 294–299, 2019, doi: 10.1109/MODELS.2019.00013.

[47] K. Khalil, B. Dey, A. Kumar, and M. Bayoumi, “A reversible-logic based architecture for long short-term memory (LSTM) network,” *Proc. - IEEE Int. Symp. Circuits Syst.*, vol. 2021-May, 2021, doi: 10.1109/ISCAS51556.2021.9401395.

[48] B. N. Saha, A. Senapati, and A. Mahajan, “LSTM based Deep RNN Architecture for Election Sentiment Analysis from Bengali Newspaper,” *2020 Int. Conf. Comput. Perform. Eval. ComPE 2020*, pp. 564–569, 2020, doi: 10.1109/ComPE49325.2020.9200062.

[49] N. Elsayed, A. S. Maida, and M. Bayoumi, “Reduced-Gate Convolutional LSTM Architecture for Next-Frame Video Prediction Using Predictive Coding,” *Proc. Int. Jt. Conf. Neural Networks*, vol. 2019-July, no. July, pp. 1–9, 2019, doi: 10.1109/IJCNN.2019.8852480.

[50] H. Zou, Y. Wu, H. Zhang, and Y. Zhan, “Short-term Traffic Flow Prediction Based on PCC-BiLSTM,” *Proc. - 2020 Int. Conf. Comput. Eng. Appl. ICCEA 2020*, pp. 489–493, 2020, doi: 10.1109/ICCEA50009.2020.00110.

[51] Z. Hameed and B. Garcia-Zapirain, “Sentiment Classification Using a Single-Layered BiLSTM Model,” *IEEE Access*, vol. 8, pp. 73992–74001, 2020, doi: 10.1109/ACCESS.2020.2988550.

[52] K. Shyamala and C. S. Padmasini, “Mtanh-Attention-BiLSTM model for prediction of Automobile Export Customer Satisfaction.,” *Proc. - Int. Conf. Artif. Intell. Smart Syst. ICAIS 2021*, pp. 652–660, 2021, doi: 10.1109/ICAIS50930.2021.9395837.

[53] 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.

[54] Muhammad Gerald Rizky, “Analisis Perbandingan Metode LSTM dan BiLSTM Untuk Klasifikasi Sinyal Jantung Phonocardiogram,” pp. 1–63, 2021, [Online]. Available: https://repository.dinamika.ac.id/id/eprint/5962/1/17410200021-2021-UNIVERSITAS DINAMIKA.pdf.

[55] G. Liu and J. Guo, “Bidirectional LSTM with attention mechanism and convolutional layer for text classification,” *Neurocomputing*, vol. 337, pp. 325–

338, 2019, doi: 10.1016/j.neucom.2019.01.078.

[56] T. E. Trueman, A. K. J., P. Narayanasamy, and J. Vidya, “Attention-based C-BiLSTM for fake news detection,” *Appl. Soft Comput.*, vol. 110, p. 107600, 2021, doi: 10.1016/j.asoc.2021.107600.

[57] K. Gao, H. Xu, C. Gao, H. Hao, J. Deng, and X. Sun, “Attention-Based BiLSTM Network with Lexical Feature for Emotion Classification,” *Proc. Int. Jt. Conf. Neural Networks*, vol. 2018-July, pp. 1–2, 2018, doi: 10.1109/IJCNN.2018.8489577.

[58] Z. Wu, “The comparison of forecasting analysis based on the ARIMA-LSTM hybrid models,” *Proc. - 2021 Int. Conf. E-Commerce E-Management, ICECEM 2021*, pp. 185–188, 2021, doi: 10.1109/ICECEM54757.2021.00044.

[59] G. Xu, Y. Meng, X. Qiu, Z. Yu, and X. Wu, “Sentiment analysis of comment texts based on BiLSTM,” *IEEE Access*, vol. 7, no. c, pp. 51522–51532, 2019, doi: 10.1109/ACCESS.2019.2909919.

[60] R. Zhao, Y. Yin, Y. Shi, and Z. Xue, “Intelligent intrusion detection based on federated learning aided long short-term memory,” *Phys. Commun.*, vol. 42, p. 101157, 2020, doi: 10.1016/j.phycom.2020.101157.

[61] Canadian institute for cyebersecurity, “CSE-CIC-IDS2018 on AWS,” *university of new brunswick*, 2018. https://www.unb.ca/cic/datasets/ids-2018.html (accessed Jul. 12, 2022).

[62] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” *ICISSP 2018 - Proc. 4th Int. Conf. Inf. Syst. Secur. Priv.*, vol. 2018-Janua, no. Cic, pp. 108–116, 2018, doi: 10.5220/0006639801080116.

[63] Z. I. Detection, “Evaluation of Machine Learning Classifiers for Zero-Day Intrusion Detection – An Analysis on CIC-AWS-2018 dataset,” 2018.

[64] S. Chormunge and S. Jena, “Correlation based feature selection with clustering for high dimensional data,” *J. Electr. Syst. Inf. Technol.*, vol. 5, no. 3, pp. 542–549, 2018, doi: 10.1016/j.jesit.2017.06.004.

[65] A. Gumilar, S. S. Prasetiyowati, and Y. Sibaroni, “Performance Analysis of Hybrid Machine Learning Methods on,” vol. 5, no. 158, pp. 481–490, 2022.

[66] S. Su, Y. Sun, X. Gao, J. Qiu, and Z. Tian, “A correlation-change based feature selection method for IoT equipment anomaly detection,” *Appl. Sci.*, vol. 9, no. 3, 2019, doi: 10.3390/app9030437.

[67] D. R. Alghifari, M. Edi, and L. Firmansyah, “Implementasi Bidirectional LSTM untuk Analisis Sentimen Terhadap Layanan Grab Indonesia Bidirectional LSTM Implementation for Sentiment Analysis Against Grab Indonesia Services,” *J. Manaj. Inform.*, vol. 12, pp. 89–99, 2022.