MULTI CLASSIFICATION PADA SISTEM PENDETEKSI SERANGAN SIBER MENGGUNAKAN LSTM VARIANT

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH:

REVI APRILIA MAHARANI

09011282025032

JURUSAN SISTEM KOMPUTER

FAKUTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

MULTI CLASSIFICATION PADA SISTEM PENDETEKSI SERANGAN SIBER MENGGUNAKAN LSTM VARIANT

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

REVI APRILIA MAHARANI

09011282025032

Indralaya, 4 Januari 2024

Mengetahui,

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

AUTHENTICATION PAGE

MULTI-CLASSIFICATION IN CYBER ATTACK DETECTION SYSTEM USING LSTM VARIANT

FINAL TASK

Submitted To Fullfill One Of The Requirments To Obtain
Obtain A Bachelor's Degree In Computer Science

By

REVI APRILIA MAHARANI
09011282025032

Indralaya, 11 January 2024

Acknowledge,

Head of Computer System Departement	Final Project Advisor
Dr. Ir. H. Sukemi, M.T.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Rabu

Tanggal : 27 Desember 2023

Tim Penguji :

1. Ketua : Ahmad Fali Oklilas, M.T.
2. Sekertaris : Iman Saladin B. Azhar, M.MSI.
3. Penguji : Huda Ubaya, M.T.
4. Pembimbing : Ahmad Heryanto, S.Kom., M.T

Mengetahui,

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

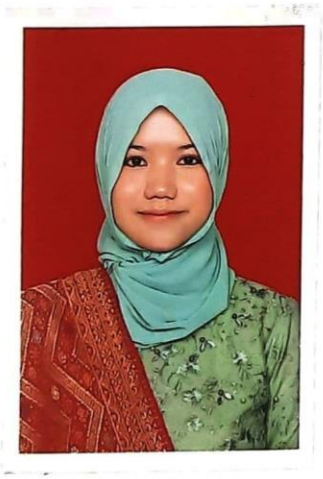
Yang bertanda tangan di bawah ini:

Nama	:	Revi Aprilia Maharani
NIM	:	09011282025032
Judul	:	Multi Classification Pada Sistem Pendeteksi Serangan Siber Menggunakan Lstm Variant

Hasil Pengecekan Software iThenticate/Turnitin : 3%

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, 11 Januari 2024

Revi Aprilia Maharani

NIM.09011282025032

KATA PENGANTAR

Puji syukur Alhamdulillah penulis panjatkan atas kehadirat Allah SWT yang telah memberikan ridho dan berkah-Nya, sehingga penulis dapat menyelesaikan penyusunan Tugas Akhir yang berjudul **"Multi Classification Pada Sistem Pendeteksi Serangan Siber Menggunakan LSTM Variant".**

Adapun selain itu penulis mengucapkan terima kasih kepada setiap orang yang telah membantu, membimbing, mendengarkan keluh kesah, dan merangkul penulis agar tetap berjuang dalam menyelesaikan penyusunan Tugas Akhir ini. Dengan demikian, pada kesempatan ini izinkan penulis untuk mengucapkan terima kasih kepada:

1. Pahlawan terfavorit sepanjang masa, ayah. Terima kasih karena tidak pernah menuntut, namun terus memberi semangat. Berkat cinta dan kasih ayah, penulis selalu merasa aman dan bahagia.
2. Wanita hebat yang telah menjadi bubun dan sahabat bagi penulis. Bubun selalu jadi pendengar disegala lembar cerita penulis, dan selalu menemani penulis di berbagai lembar ceritanya. 24/7 penulis membutuhkan, bubun selalu ada. Terima kasih bubun atas cinta dan kasih yang bubun berikan, berkat bubun penulis dapat terus melangkah ke lembar-lembar berikutnya dengan penuh senyuman.
3. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
4. Bapak Dr. Firdaus, M.KOM., selaku dosen Pembimbing Akademik.
5. Bapak Ahmad Heryanto, S.Kom., M.T., selaku dosen Pembimbing Skripsi yang telah sangat baik kepada penulis. Bapak selalu ada membantu diberbagai jalan buntu dari lembar cerita tugas akhir ini, tentunya penulis amat sangat berterima kasih dan bersyukur karena telah menjadi anak bimbingan bapak,
6. Sosok yang selalu ada dalam tiap lembar cerita penulis dalam beberapa tahun ini, Muhammad Ridho cahyo. Abang yang selalu ada, menemani, dan membantu penulis dalam berbagai lembar cerita ini, membuat penulis amat sangat bersyukur dapat mengenal abang.

7. Adik kesayangan penulis, si bocil menyebalkan namun penuh perhatian yang selalu memberikan kasih sayangnya kepada penulis.
8. Wak ibuk, wak aba, kak Bugis, dan kak Rey, yang penulis sayangi.
9. Kepada teman-teman kelas SKB 2020 dan teman-teman di lab comnets.
10. Geng MC yang telah menjadi teman seperpusingan dalam mengejar akurasi.
11. Umintet dan Patam yang selalu jadi tempat penulis dalam menghilangkan penat perkuliahan.
12. Thalia dan Dips yang suka ribut namun dapat membuat penulis gembira.
13. Infinite yang selalu menyenangkan dan anak-anak PPSDM yang *super* gemes.
14. Lingkungan pertemanan yang pernah ada dalam berbagai cerita penulis di masa perkuliahan.
15. 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 Tugas Akhir ini dapat bermanfaat serta dapat memberikan pengetahuan dan wawasan bagi semua pihak yang membutuhkannya. Khususnya mahasiswa/i Jurusan Sistem Komputer Universitas Sriwijaya.

Penulis,

Revi Aprilia Maharani
NIM. 09011282025032

MULTI CLASSIFICATION PADA SISTEM PENDETEKSI SERANGAN SIBER MENGGUNAKAN LSTM VARIANT

REVI APRILIA MAHARANI
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : reviapriliamaharani@gmail.com

ABSTRAK

Long Short Term Memory, metode pendeteksi serangan siber dengan kemampuan memproses urutan data dan mengingat informasi dalam rentang waktu panjang. Namun, LSTM tidak dapat secara efektif mengingat informasi apabila urutan data terlalu panjang atau informasi tersebar pada jarak yang jauh. Oleh karena itu, hadir metode Bidirectional LSTM dan Stacked LSTM. BiLSTM mampu memproses urutan data secara simultan ke depan dan ke belakang, sehingga mampu menangkap konteks global dari data dan dapat memproses urutan data yang kompleks. Stacked LSTM, terdiri dari beberapa lapisan LSTM yang ditumpuk secara berurutan, sehingga mampu mendeteksi serangan siber dengan urutan data yang sangat panjang dan bervariasi. Penelitian ini mengidentifikasi metode yang paling efektif dalam klasifikasi serangan siber pada dataset multiclass, dengan mempertimbangkan kompleksitas dan karakteristik dataset CIC-IDS-2018, ISCXIDS2012, KDD Cup 1999, dan NSL-KDD. Validasi terbaik pada CIC-IDS-2018, Stacked LSTM dengan akurasi sebesar 86.99%. Pada ICXIDS2012, metode Stacked LSTM dengan akurasi 99.38%. Dataset KDD Cup 1999, Bidirectional LSTM dengan akurasi 99.08%. Pada dataset NSL-KDD, Bidirectional LSTM dengan akurasi 95.14%.

Kata kunci : LSTM, Stacked LSTM, Bidirectional LSTM

Mengetahui,

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

MULTI-CLASSIFICATION IN CYBER ATTACK DETECTION SYSTEM USING LSTM VARIANT

REVI APRILIA MAHARANI
Departement of Computer System, Faculty of Computer Science, Sriwijaya University
Email : reviapriliamaharani@gmail.com

ABSTRACT

Long Short-Term Memory (LSTM) is a method for detecting cyber attacks with the ability to process sequential data and remember information over a long period of time. However, LSTM may not effectively retain information when the data sequence is too long or when information is widely dispersed. Therefore, the bidirectional LSTM and stacked LSTM methods are introduced. BiLSTM can process sequential data simultaneously in both forward and backward directions, capturing the global context of the data and handling complex data sequences. Stacked LSTM consists of multiple layers of sequentially stacked LSTMs, allowing it to detect cyber attacks in very long and varied data sequences. This research identifies the most effective methods for classifying cyber attacks in multiclass datasets, taking into consideration the complexity and characteristics of the CIC-IDS-2018, ISCXIDS2012, KDD Cup 1999, and NSL-KDD datasets. The best validation results were obtained on the CIC-IDS-2018 dataset, with stacked LSTM achieving an accuracy of 86.99%. For ICXIDS 2012, the stacked LSTM method achieved an accuracy of 99.38%. In the KDD Cup 1999 dataset, bidirectional LSTM achieved an accuracy of 99.08%. Lastly, for the NSL-KDD dataset, bidirectional LSTM also achieved an accuracy of 95.14%.

Keywords : LSTM, Stacked LSTM, Bidirectional LSTM

Acknowledge,

Head of Computer System Departement	**Final Project Advisor,**
Dr. Ir. H. Sukemi, M.T.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1. Latar Belakang

Serangan siber merupakan kejahatan yang dilakukan oleh individu atau organisasi, dengan tujuan merusak ataupun mendapatkan akses pada dokumen dan sistem penting dalam jaringan komputer, baik dalam hal bisnis ataupun pribadi guna menghancurkan atau mendapatkan akses mengenai informasi rahasia[1]. Dalam penggunaan internet terdapat berbagai jenis serangan siber seperti yang akan dibahas pada penelitian ini diantaranya yaitu, *Bruteforce attack*, *DoS attack*, *DDoS attack*, *Heartbleed*, *Botnet*, *Web attack*, *infiltration attack*, dan lain sebagainya.

Dalam mendeteksi serangan siber terdapat berbagai metode yang digunakan dalam penelitian, seperti halnya pada penelitian[2] yang menggunakan metode *Naive Bayes*, metode ini berdasarkan teorema *Bayes* dengan mengklasifikasikan data ke dalam kelas yang telah ditentukan berdasarkan oleh fitur-fitur yang diberikan, sehingga berguna dalam tugas klasifikasi yang terdapat beberapa fitur relevan guna memprediksi kelas target. Namun pada *Naive Bayes* asumsi independensinya kuat antara fitur-fitur, dengan begitu asumsi ini sering kali tidak realistis dalam banyak dataset karena banyaknya ketergantungan yang ada antara fitur-fitur tertentu. Selain itu kemampuan *Naive Bayes* kurang dalam memproses data teks atau urutan, dimana metode ini berkemungkinan tidak dapat memanfaatkan ketergantungan antara kata atau elemen dalam urutan, sehingga *Naive Bayes* lebih cocok untuk data tabular atau data dengan fitur-fitur independent. Lalu selanjutnya pada penelitian[3]menggunakan metode *KNN* (*K-Nearest Neighbors*) yang merupakan metode pembelajaran mesin pada penggunaan klasifikasi dan regresi, pada dasarnya *KNN* ialah metode sederhana yang memprediksi kelas atau nilai suatu data baru dengan berdasarkan mayoritas kelas atau nilai dari “tetangga terdekat” dalam ruang fitur, namun sayangnya metode ini cenderung sensitif terhadap data noise dan outliers dikarenakan prediksi

berdasarkan “tetangga terdekat” dapat terpengaruhi oleh data yang tidak biasa ataupun tidak representative. Serta terdapat metode *SVM* (*Support Vector Machine*) yang digunakan pada penelitian[4], *SVM* ialah metode yang digunakan dalam pengklasifikasian dan regresi, dengan fungsinya dalam mencari hyperplane terbaik yang mampu memisahkan dua kelas dalam ruang fitur, namun *SVM* memiliki kekurangan dimana proses pelatihan *SVM* memakan waktu yang signifikan, terutama ketika jumlah sampel atau dimensi fitur sangat besar.

Berdasarkan penjabaran dari beberapa metode diatas, setiap kelemahan tersebut mampu diatasi oleh metode *Long Short Therm Memory* (*LSTM*) *variant*. Seperti halnya *Bidirectional LSTM (BI-LSTM*) yang dirancang khusus guna memahami dan menangkap ketergantungan temporal dalam data urutan. Dimana dengan kemampuan memori jangka panjang dan pengenalan pola yang kompleks, varian dari *LSTM* ini mampu mengidentifikasi ketergantungan antara fitur-fitur yang tidak dapat ditangkap oleh *Naive Bayes*, pun mampu memberikan kinerja yang lebih baik dalam pengolahan data teks atau urutan[5]. Varian-varian *LSTM* juga mampu mengatasi kelemahan akan sensitivitas terhadap *noise* dan *outlier*s pada *KNN*, dengan memproses data urutan dan mengenali pola pola temporal. Dengan demikian, apabila data noise atau outlier muncul, varian *LSTM* mampu mengabaikan dampak ataupun memperlakukan mereka sebagai bagian dari pola yang besar[6]. Varian dari *LSTM* juga memiliki arsitektur yang lebih terstruktur dan lebih sederhana dibandingan *SVM*, sehingga waktu pelatihan *LSTM* dalam beberapa kasus dapat lebih efisien dibandingkan *SVM*[7].

Long Short Therm Memory (*LSTM*) yang merupakan jenis arsitektur jaringan saraf tiruan yang berguna dalam mendeteksi serangan siber dikarenakan kemampuannya dalam memproses urutan data dengan baik dan mengatasi masalah vanishing gradient yang sering terjadi pada arsitektur jaringan saraf yang lebih sederhana[8]. Selain itu, *LSTM* juga mampu mengingat informasi dalam rentang waktu yang panjang, serta mampu menghapus informasi yang tidak efektif. *LSTM* memiliki karakteristik yaitu sebuah jaringan khusus dari jenis *RNN*, yang dapat mempelajari dependensi dalam jangka Panjang[9]. Dengan berbagai keunggulan *LSTM*, tentunya tidak luput dari kelemahan, dimana meskipun *LSTM* dirancang

guna mempertahankan informasi jangka panjang, *LSTM* juga tidak dapat secara efektif mengingat informasi yang relevan, apabila urutan datanya terlalu panjang atau informasi relevan tersebar di seluruh urutan dengan jarak yang jauh[10].

Dengan kekurangan yang terdapat pada *LSTM*, pada penelitian ini digunakan *Bidirectional Long Short Term Memory (Bi-LSTM*), dikarenakan Bi-*LSTM* memiliki kemampuan dalam memproses urutan data secara simultan ke depan dan ke belakang (dua arah), yang memungkinkan model untuk lebih baik dalam menangkap konteks global dari data, menjadi lebih responsif terhadap pola-pola yang dapat muncul dari berbagai arah, sehingga dapat memproses urutan data yang kompleks[11]. Selain kedua metode sebelumnya, digunakan juga metode *Stacked LSTM*, yang merupakan arsitektur jaringan saraf yang terdiri dari beberapa lapisan *LSTM* yang ditumpuk secara berurutan. *Stacked LSTM* digunakan karena kemampuannya dapat efektif mendeteksi serangan siber dengan urutan data yang panjang dan bervariasi[12].

Dalam penelitian[13] membahas mengenai penggunaan *Bidirectional LSTM d*alam meningkatkan kinerja *IDS* dalam pada keamanan cyber, dengan *akurasi* sebesar 99.94%. Lalu[14] yang melakukan penelitian pada *Bidirectional LSTM m*enggunakan dataset *UNSW-NB15* dan *KDD Cup 1999* mendapatkan *akurasi* sebesar 99.70%. Selanjutnya[12] pada yang berisikan penelitian dengan menggunakan *Stacked LSTM* dan *Bidirectional LSTM p*ada dataset *UNSWNB15* memiliki *akurasi* sebesar 96.60% dan 96.41%.

Berdasarkan penjabaran tersebut, maka penulis akan melakukan penelitian mengenai multi classification pada sistem pendeteksi serangan siber menggunakan *LSTM* variant (*LSTM, BiLSTM,* dan *Stacked LSTM).* Metode *LSTM* tidak dapat secara efektif mengingat informasi yang relevan apabila urutan datanya terlalu panjang atau informasi relevan tersebar di seluruh urutan dengan jarak yang jauh. Sebaliknya, *BiLSTM* mengatasi kendala tersebut dengan memproses data dari kedua arah, memungkinkan model untuk lebih baik dalam menangkap konteks global dari data yang kompleks. *Stacked LSTM,* dengan keunggulan representasi yang kompleks melalui beberapa lapisan, mampu mengatasi urutan data yang sangat panjang. Oleh karena itu, penelitian ini diarahkan untuk mengidentifikasi

metode yang paling efektif dalam konteks klasifikasi serangan siber, dengan mempertimbangkan kompleksitas dan karakteristik data yang dihadapi, yaitu *dataset CIC-IDS-2018, ISCXIDS2012, KDD Cup 1999,* dan *NSL-KDD.*

1.2. Perumusan Masalah

Berikut ini beberapa rumusan masalah dalam melaksanakan penelitian Tugas Akhir ini, yaitu:

1. Bagaimana pengoptimalan *LSTM variant* (*LSTM, BiLSTM,* dan *Stacked LSTM)* dalam mendeteksi serangan siber pada klasifikasi *multiclassification*?
2. Berdasarkan empat dataset yang digunakan (*CIC-IDS-2018, ISCXIDS2012, KDD Cup 1999,* dan *NSL-KDD*), metode manakah yang memiliki hasil terbaik berdasarkan beberapa nilai yaitu *akurasi, recall, presisi, spesifitas,* dan *F1-Score?*
3. Apakah hasil pengujian menggunakan empat dataset tersebut menunjukkan konsistensi peningkatan kinerja metode *Bidirectional LSTM* dan *Stacked LSTM* dibandingkan dengan metode *LSTM*?

1.3. Batasan Masalah

Berdasarkan rumusan masalah di atas, adapun batasan masalah yang terdapat dalam penyusunan tugas akhir ini, yaitu:

1. Dataset yang digunakan dalam penelitian ini ialah dataset yang berisikan lebih dari 2 kelas yaitu *CIC-IDS 2018, ISCXIDS2012, KDD Cup 1999,* dan *NSL-KDD.*
2. Penelitian ini menghasilkan output bebupa beberapa nilai *yaitu akurasi, recall, spesifitas, presisi,* dan *F1-Score* sebagai tolak ukur.

1.4. Tujuan

Berdasarkan penelitian yang dilakukan, adapun tujuan dari penelitian Tugas Akhir ini yaitu:

1. Untuk menerapkan *multiclassification* dalam mendeteksi serangan siber menggunakan metode *LSTM, Bidirectional LSTM,* dan *Stacked LSTM*.

2. Guna membandingkan hasil terbaik yang didapatkan oleh metode *LSTM, Bidirectional LSTM,* dan *Stacked LSTM* dalam pengujian dengan menggunakan dataset *CIC-IDS 2018, ISCXIDS2012, KDD Cup 1999,* dan *NSL-KDD*, berdasarkan performa hasil dari kinerja penelitian terhadap beberapa nilai yaitu *akurasi*, *recall*, *presisi*, *spesifitas*, dan *F1-Score*.
3. Untuk melihat peningkatan kinerja metode Bidirectional LSTM dan Stacked LSTM dibandingkan dengan metode LSTM menggunakan empat dataset.

1.5. Manfaat

Berdasarkan penelitian yang dilakukan, adapun manfaat dari penelitian Tugas Akhir ini, yaitu:

1. Dapat memahami bagaimana penerapan metode *LSTM*, *Bidirectional LSTM*, dan *Stacked LSTM* dalam mendeteksi beberapa jenis serangan siber pada dataset *multiclass*.
2. Dapat mengetahui bagaimana hasil kinerja yang dilakukan oleh metode *LSTM*, *Bidirectional LSTM,* dan *Stacked LSTM* dalam pengujian beberapa dataset yang karakteristiknya berbeda.

1.6. Sistematika Penulisan

Untuk dapat mempermudah dan memperjelas proses penyusunan Tugas Akhir ini, dibuat sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisikan penjelasan secara sistematis berupa topik penelitian yang berisikan latar belakang, tujuan, manfaat, perumusan masalah, Batasan masalah, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisikan penjelasan dasar teori dari penelitian mengenai serangan siber.

BAB III METODOLOGI PENELITIAN

Pada bab ketiga, membahas proses yang dilakukan dalam penelitian

secara sistematis. Serta mengkaji tahapan perancangan sistem, dan penerapan dari metode penelitian.

BAB IV HASIL DAN ANALISA

Bab ini menjelaskan hasil dari proses pengujian yang telah dilakukan, dan melakukan analisis data yang didapat dari hasil pengujian.

BAB V KESIMPULAN DAN SARAN

Pada bab terakhir, berisikan kesimpulan dan saran dari hasil analisa berdasarkan penelitian yang telah dilakukan.

DAFTAR PUSTAKA

[1] E. Susanto, Lady Antira, K. Kevin, E. Stanzah, and A. A. Majid, "Manajemen Keamanan Cyber di Era Digital," *Journal of Business And Entrepreneurship*, vol. 11, no. 1, pp. 23–33, 2023.

[2] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, "A bidirectional LSTM deep learning approach for intrusion detection," *Expert Syst Appl*, vol. 185, p. 115524, 2021.

[3] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, "A DDoS attack mitigation framework for IoT networks using fog computing," *Procedia Comput Sci*, vol. 182, pp. 13–20, 2021.

[4] M. Azizjon, A. Jumabek, and W. Kim, "1D CNN based network intrusion detection with normalization on imbalanced data," in *2020 international conference on artificial intelligence in information and communication (ICAIIC)*, IEEE, 2020, pp. 218–224.

[5] Z. Geng, G. Chen, Y. Han, G. Lu, and F. Li, "Semantic relation extraction using sequential and tree-structured LSTM with attention," *Inf Sci (N Y)*, vol. 509, pp. 183–192, 2020.

[6] F. Kulsoom, S. Narejo, Z. Mehmood, H. N. Chaudhry, A. Butt, and A. K. Bashir, "A review of machine learning-based human activity recognition for diverse applications," *Neural Comput Appl*, vol. 34, no. 21, pp. 18289–18324, 2022.

[7] S. Gangwar, V. Bali, and A. Kumar, "Comparative analysis of wind speed forecasting using LSTM and SVM," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 7, no. 25, pp. e1–e1, 2020.

[8] S. Sivamohan, S. S. Sridhar, and S. Krishnaveni, "An effective recurrent neural network (RNN) based intrusion detection via bi-directional long short-term memory," in *2021 international conference on intelligent technologies (CONIT)*, IEEE, 2021, pp. 1–5.

[9] A. U. Rehman, A. K. Malik, B. Raza, and W. Ali, "A hybrid CNN-LSTM model for improving accuracy of movie reviews sentiment analysis,"

Multimed Tools Appl, vol. 78, pp. 26597–26613, 2019.

[10] S. Al-Selwi, M. Hassan, S. Jadid Abdulkadir, and A. Muneer, "LSTM Inefficiency in Long-Term Dependencies Regression Problems," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 30, pp. 16–31, May 2023, doi: 10.37934/araset.30.3.1631.

[11] H. Jahangir, H. Tayarani, S. S. Gougheri, M. A. Golkar, A. Ahmadian, and A. Elkamel, "Deep learning-based forecasting approach in smart grids with microclustering and bidirectional LSTM network," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 9, pp. 8298–8309, 2020.

[12] K. Saurabh *et al.*, "Lbdmids: LSTM based deep learning model for intrusion detection systems for IOT networks," in *2022 IEEE World AI IoT Congress (AIIoT)*, IEEE, 2022, pp. 753–759.

[13] N. Oliveira, I. Praça, E. Maia, and O. Sousa, "Intelligent cyber attack detection and classification for network-based intrusion detection systems," *Applied Sciences*, vol. 11, no. 4, p. 1674, 2021.

[14] T. S. Pooja and P. Shrinivasacharya, "Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 448–454, 2021.

[15] S. Pillai and A. Sharma, "Hybrid unsupervised web-attack detection and classification–A deep learning approach," *Comput Stand Interfaces*, vol. 86, p. 103738, 2023.

[16] W. Lo, H. Alqahtani, K. Thakur, A. Almadhor, S. Chander, and G. Kumar, "A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic," *Vehicular Communications*, vol. 35, p. 100471, 2022.

[17] E. Mushtaq, A. Zameer, M. Umer, and A. A. Abbasi, "A two-stage intrusion detection system with auto-encoder and LSTMs," *Appl Soft Comput*, vol. 121, p. 108768, 2022.

[18] M. I. Sayed, I. M. Sayem, S. Saha, and A. Haque, "A Multi-Classifier for DDoS Attacks Using Stacking Ensemble Deep Neural Network," in *2022 International Wireless Communications and Mobile Computing (IWCMC)*, IEEE, 2022, pp. 1125–1130.

[19] B. I. Farhan and A. D. Jasim, “Performance analysis of intrusion detection for deep learning model based on CSE-CIC-IDS2018 dataset,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 2, pp. 1165–1172, 2022.

[20] A. A. Hagar and B. W. Gawali, “Deep Learning for Improving Attack Detection System Using CSE-CICIDS-2018,” *NeuroQuantology*, 2022.

[21] A. Ozcan, C. Catal, E. Donmez, and B. Senturk, “A hybrid DNN–LSTM model for detecting phishing URLs,” *Neural Comput Appl*, pp. 1–17, 2021.

[22] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, “A DDoS attack mitigation framework for IoT networks using fog computing,” *Procedia Comput Sci*, vol. 182, pp. 13–20, 2021.

[23] G. C. Amaizu, C. I. Nwakanma, S. Bhardwaj, J. M. Lee, and D.-S. Kim, “Composite and efficient DDoS attack detection framework for B5G networks,” *Computer Networks*, vol. 188, p. 107871, 2021.

[24] O. M. A. Alsyaibani, E. Utami, and A. D. Hartanto, “An Intrusion Detection System Model Based on Bidirectional LSTM,” in *2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS)*, IEEE, 2021, pp. 1–6.

[25] O. M. A. Alsyaibani, E. Utami, and A. D. Hartanto, “An Intrusion Detection System Model Based on Bidirectional LSTM,” in *2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS)*, IEEE, 2021, pp. 1–6.

[26] 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,” in *2020 5th international conference on computer and communication systems (ICCCS)*, IEEE, 2020, pp. 491–497.

[27] F. Ertam, “An efficient hybrid deep learning approach for internet security,” *Physica A: Statistical Mechanics and Its Applications*, vol. 535, p. 122492, 2019.

[28] J. M. Olamantanmi, O. D. Alowolodu, J. O. Mebawondu, and A. O. Adetunmbi, “Network Intrusion Detection System using Supervised Learning Paradigm,” *Sci Afr*, vol. 10, 2020.

[29] A. Jeronimo, “The Globalization Effect Of Law And Economic On Cybercrime,” *Jurnal Pembaharuan Hukum THE GLOBALIZATION EFFECT OF LAW AND*, vol. 6, no. 3, pp. 12–27, 2019.

[30] S. A. M. Babys, “Ancaman Perang Siber Di Era Digital Dan Solusi Keamanan Nasional Indonesia,” *Oratio Directa (Prodi Ilmu Komunikasi)*, vol. 3, no. 1, 2021.

[31] N. Vugdelija, N. Nedeljković, N. Kojić, L. Lukić, and M. Vesić, “Review of brute-force attack and protection techniques,” in *13th International Conference, ICT Innovations 2021*, 2021, pp. 220–230.

[32] A. Huseinović, S. Mrdović, K. Bicakci, and S. Uludag, “A survey of denial-of-service attacks and solutions in the smart grid,” *IEEE Access*, vol. 8, pp. 177447–177470, 2020.

[33] M. M. Salim, S. Rathore, and J. H. Park, “Distributed denial of service attacks and its defenses in IoT: a survey,” *J Supercomput*, vol. 76, pp. 5320–5363, 2020.

[34] R. Abubakar *et al.*, “An effective mechanism to mitigate real-time DDoS attack,” *IEEE Access*, vol. 8, pp. 126215–126227, 2020.

[35] Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, “A distributed deep learning system for web attack detection on edge devices,” *IEEE Trans Industr Inform*, vol. 16, no. 3, pp. 1963–1971, 2019.

[36] Z. Bederna and T. Szadeczky, “Cyber espionage through Botnets,” *Security Journal*, vol. 33, no. 1, pp. 43–62, 2020.

[37] B. Al-Duwairi and M. Jarrah, “Botnet Architectures,” *Botnets: Architectures, Countermeasures, and Challenges*, vol. 1, 2019.

[38] A. Arora, S. K. Yadav, and K. Sharma, “Denial-of-service (dos) attack and botnet: Network analysis, research tactics, and mitigation,” in *Research Anthology on Combating Denial-of-Service Attacks*, IGI Global, 2021, pp. 49–73.

[39] P. Kumar, G. P. Gupta, and R. Tripathi, “Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for iot networks,” *Arab J Sci Eng*, vol. 46, pp. 3749–3778, 2021.

[40] O. Alkadi, N. Moustafa, and B. Turnbull, “A review of intrusion detection

and blockchain applications in the cloud: approaches, challenges and solutions," *IEEE Access*, vol. 8, pp. 104893–104917, 2020.

[41] M. Usama, M. Asim, S. Latif, and J. Qadir, "Generative adversarial networks for launching and thwarting adversarial attacks on network intrusion detection systems," in *2019 15th international wireless communications & mobile computing conference (IWCMC)*, IEEE, 2019, pp. 78–83.

[42] A. S. Bhadouria, "Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World's Biggest Data Breaches," *International Journal of Scientific and Research Publications*, 2022.

[43] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, 2019.

[44] Y. E. L. Mourabit, A. Toumanari, A. Bouirden, H. Zougagh, and R. Latif, "Intrusion detection system in Wireless Sensor Network based on mobile agent," in *2014 Second World Conference on Complex Systems (WCCS)*, IEEE, 2014, pp. 248–251.

[45] S. Al and M. Dener, "STL-HDL: A new hybrid network intrusion detection system for imbalanced dataset on big data environment," *Comput Secur*, vol. 110, p. 102435, 2021.

[46] P. Del Moral, S. Nowaczyk, and S. Pashami, "Why is multiclass classification hard?," *IEEE Access*, vol. 10, pp. 80448–80462, 2022.

[47] S. Raschka, J. Patterson, and C. Nolet, "Machine learning in python: Main developments and technology trends in data science, machine learning, and artificial intelligence," *Information*, vol. 11, no. 4, p. 193, 2020.

[48] Q. Wang, R.-Q. Peng, J.-Q. Wang, Z. Li, and H.-B. Qu, "NEWLSTM: An optimized long short-term memory language model for sequence prediction," *IEEE Access*, vol. 8, pp. 65395–65401, 2020.

[49] R. C. Staudemeyer and E. R. Morris, "Understanding LSTM--a tutorial into long short-term memory recurrent neural networks," *arXiv preprint arXiv:1909.09586*, 2019.

[50] R. Zhao, Y. Yin, Y. Shi, and Z. Xue, "Intelligent intrusion detection based

on federated learning aided long short-term memory," *Physical Communication,* vol. 42, p. 101157, 2020.

[51] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in *International Conference on Information Systems Security and Privacy*, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:4707749

[52] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Comput Secur*, vol. 31, no. 3, pp. 357–374, 2012, doi: https://doi.org/10.1016/j.cose.2011.12.012.

[53] S. Kumar, Sunanda, and S. Arora, "A statistical analysis on KDD Cup'99 dataset for the network intrusion detection system," *Applied Soft Computing and Communication Networks: Proceedings of ACN 2019*, pp. 131–157, 2020.

[54] A. Thakkar and R. Lohiya, "A review of the advancement in intrusion detection datasets," *Procedia Comput Sci*, vol. 167, pp. 636–645, 2020.

[55] S. Chormunge and S. Jena, "Correlation based feature selection with clustering for high dimensional data," *Journal of Electrical Systems and Information Technology*, vol. 5, no. 3, pp. 542–549, 2018.

[56] S. Su, Y. Sun, X. Gao, J. Qiu, and Z. Tian, "A correlation-change based feature selection method for IoT equipment anomaly detection," *Applied sciences*, vol. 9, no. 3, p. 437, 2019.

[57] E. Y. Güven, S. Gülgün, C. Manav, B. Bakır, and Z. G. Aydın, "Multiple Classification of Cyber Attacks Using Machine Learning," *Electrica*, vol. 22, no. 2, pp. 313–320, 2022.

[58] T. Kim and W. Pak, "Hybrid classification for high-speed and high-accuracy network intrusion detection system," *IEEE Access*, vol. 9, pp. 83806–83817, 2021.

[59] H. Alqahtani, I. H. Sarker, A. Kalim, S. M. Minhaz Hossain, S. Ikhlaq, and S. Hossain, "Cyber intrusion detection using machine learning classification techniques," in *Computing Science, Communication and Security: First*

International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1, Springer, 2020, pp. 121–131.

[60] H. Hou *et al.*, "Hierarchical long short-term memory network for cyberattack detection," *IEEE Access*, vol. 8, pp. 90907–90913, 2020.