DETEKSI SERANGAN MIRAI DENGAN MENGGUNAKAN METODE LONG SHORT-TERM MEMORY (LSTM) PADA JARINGAN IOT

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

THALIA PUTRI

09011282025092

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

LEMBAR PENGESAHAN

DETEKSI SERANGAN MIRAI DENGAN MENGGUNAKAN METODE LONG SHORT TERM MEMORY (LSTM) PADA JARINGAN IOT

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH:

THALIA PUTRI
09011282025092

Palembang, 16 Januari 2025

Pembimbing I	**Pembimbing II**
Prof. Ir. Deris Stiawan, M.T., Ph.D.	**Nurul Afifah, M.Kom**
NIP. 197806172006041002	**NIP. 199211102023212049**

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi.M.T.
NIP.196612032006041001

ii

AUTHENTICATION PAGE

MIRAI ATTACK DETECTION USING LONG SHORT-TERM MEMORY (LSTM) METHOD ON IOT NETWORKS

THESIS

Submitted To Complete One Of The Requirements For Obtaining A Bachelor's Degree in Computer Science

By:

Thalia Putri

09011282025092

Palembang, 16 January 2025

Supervisor	Co-Superviser
Prof. Ir. Deris Stiawan, M.T., Ph.D.	**Nurul Afifah, M.Kom**
NIP. 197806172006041002	**NIP. 199211102023212049**

Acknowledge,
Head of Computer Systems Department

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

iii

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Senin

Tanggal : 23 Desember 2024

Tim Penguji :

1. **Ketua : Aditya Putra Perdana Prasetyo, S.Kom., M.T**
2. **Penguji : Huda Ubaya, M.T.**
3. **Pembimbing I : Prof. Ir. Deris Stiawan, M.T., Ph.D.**
4. **Pembimbing II : Nurul Afifah, M.Kom**

Mengetahui, 6/1/25
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

iv

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Thalia Putri

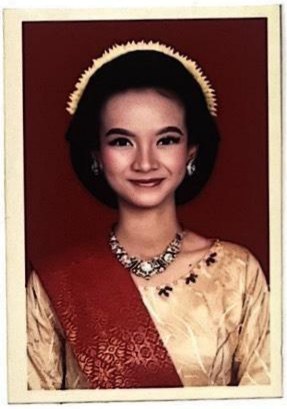
NIM : 09011282025092

Judul : Deteksi Serangan Mirai dengan Menggunakan Metode *Long Short-Term Memory* (LSTM) pada Jaringan IoT

Hasil Pengecekan Software Thenticate/Turnitin: 7%

Menyatakan bahwa laporan akhir saya meruakan 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 tanpa paksaan dari siapapun.



Palembang, 16 Januari 2025

Thalia Putri

NIM. 09011282025092

v

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji syukur Alhamdulillah penulis panjatkan atas kehadirat Allah Subhanahu Wa Ta'ala yang telah memberikan karunia dan rahmat-Nya, sehingga penulis dapat menyelesaikan penulisan skripsi berjudul **"Deteksi Serangan Mirai dengan Menggunakan metode Long Short Term Memory (LSTM) pada jaringan IoT"**. Sebagai salah satu syarat untuk meraih gelar sarjana komputer dalam bidang studi Sistem Komputer di Fakultas Ilmu Komputer.

Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada beberapa pihak atas ide dan saran serta bantuannya dalam menyelesaikan penulisan skripsi ini. Oleh karena itu, penulis ingin mengucapkan rasa syukur kepada Allah SWT dan dengan penuh hormat serta kerendahan hati, penulis ingin mengucapkan terimakasih dan penghargaan kepada :

1. Orang tua saya tercinta Ibu **Marini** yang selalu mendo'akan, mendukung serta memotivasi penulis, Bapak **Suradi Ariyanto** yang selalu berusaha dan tidak pernah menyerah. Terimakasih telah membesarkan saya dengan penuh kasih sayang dan selalu mengajarkan saya dalam berbuat hal yang baik. Terimakasih karena telah mendidik, menasehati, memberikan dukungan dukungan yang penuh dan pengorbanan yang tak ternilai harganya baik moril, materil maupun spiritual selama ini. Saudara dan Saudariku, **Habibie Dwi Putra, Radithya Tri Putra, Azizah Al - Qafi'ah, M. Dzaky Saquel,** dan **M. Arkhan Agantha** yang selalu mendukung dengan caranya dan terima kasih telah bertahan hingga detik ini. **Difa Pusparani** yang sudah penulis anggap sebagai saudari, terimakasih telah selalu bersedia untuk selalu ada. Terima kasih untuk kasih sayang, dukungan, dan motivasi yang telah diberikan.
2. Bapak Prof. Dr. Dr. Erwin, S.SI, M.SI., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

4. Bapak Prof. Ir. Deris Stiawan, M.T. selaku Dosen Pembimbing Utama yang telah bersedia meluangkan waktu untuk membimbing, mengarahkan, serta banyak memberikan ide, nasihat dan motivasi serta kritik dan saran yang sangat berarti agar penulis dapat menyelesaikan skripsi dengan baik dan benar.
5. Ibu Nurul Afifah, M.Kom selaku Dosen Pembimbing Kedua yang selalu sabar, penuh perhatian dan juga telah bersedia meluangkan waktu untuk membimbing, mengarahkan, serta banyak memberikan ide, nasihat dan motivasi serta kritik dan saran yang sangat berarti agar penulis dapat menyelesaikan skripsi dengan baik dan benar.
6. Bapak Muhammad Ali Buchari, M.T Pembimbing Akademik Jurusan Sistem Komputer.
7. Mba Renny Virgasari, Pak Yopi serta Kak M. Angga Pratama selaku admin jurusan Sistem Komputer Universitas Sriwijaya yang telah membantu proses administrasi selama mengurus perkuliahan ini.
8. Teman – teman Sistem Komputer 2020 yang turut menjadi *support system* penulis dalam menyelesaikan Tugas Akhir ini.
9. Segala pihak yang tidak dapat disebutkan satu persatu oleh penulis, diharapkan mendapatkan balasan terbaik dari Allah SWT atas segala kebaikan yang telah diberikan

Semoga penelitian ini dapat bermanfaat dalam peningkatan pengetahuan baik untuk Mahasiswa/I Jurusan Sistem Komputer FASILKOM Universitas Sriwijaya, serta semua pihak yang membutuhkannya.

Palembang, Januari 2025

Penulis,

Thalia Putri
NIM. 09011282025092

DETEKSI SERANGAN MIRAI DENGAN MENGGUNAKAN METODE LONG SHORT-TERM MEMORY (LSTM) PADA JARINGAN IOT

Thalia Putri (09011282025092)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email: thaliaputriii8@gmail.com

ABSTRAK

Perkembangan jaringan Internet of Things (IoT) telah membawa dampak signifikan pada berbagai sektor, termasuk transportasi dan pelayanan kesehatan. Namun, lonjakan adopsi IoT juga memunculkan tantangan keamanan, terutama ancaman serangan siber seperti Mirai, yang menyerang perangkat IoT melalui Distributed Denial of Service (DDoS). Berbagai metode telah dikembangkan untuk mendeteksi serangan ini, seperti blockchain, K-Nearest Neighbors (KNN), dan Support Vector Machine (SVM), namun masing-masing memiliki keterbatasan. Long Short-Term Memory (LSTM) menjadi pilihan dalam penelitian ini karena kemampuannya dalam mengolah data sekuensial dengan tingkat akurasi tinggi dan mengatasi masalah vanishing gradient. Penelitian ini berfokus pada deteksi serangan Mirai menggunakan metode LSTM pada dataset CIC IoT 2023 untuk menghasilkan solusi yang efektif dan akurat dalam mengidentifikasi ancaman.

Kata Kunci: Internet of Things (IoT), serangan Mirai, DDoS, keamanan siber, Long Short-Term Memory (LSTM), deteksi serangan.

MIRAI ATTACK DETECTION USING LONG SHORT-TERM MEMORY (LSTM) METHOD ON IOT NETWORKS

Thalia Putri (09011282025092)

Dept. of Computer System, Faculty of Computer Science, Universitas Sriwijaya

Email : thaliaputriii8@gmail.com

ABSTRACT

The development of the Internet of Things (IoT) network has had a significant impact on various sectors, including transportation and healthcare. However, the surge in IoT adoption has also raised security challenges, especially the threat of cyber attacks such as Mirai, which attacks IoT devices through Distributed Denial of Service (DDoS). Various methods have been developed to detect these attacks, such as blockchain, K-Nearest Neighbors (KNN), and Support Vector Machine (SVM), but each has its limitations. Long Short-Term Memory (LSTM) is the choice in this study because of its ability to process sequential data with a high level of accuracy and overcome the vanishing gradient problem. This study focuses on detecting Mirai attacks using the LSTM method on the CIC IoT 2023 dataset to produce an effective and accurate solution in identifying threats.

Keywords: Internet of Things (IoT), Mirai attacks, DDoS, cybersecurity, Long Short-Term Memory (LSTM), attack detection.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Peran penting jaringan *Internet of Things* (IoT) dalam kehidupan masyarakat sangat terlihat, membuka peluang baru dan memberikan dampak positif yang signifikan pada berbagai industri global. Terutama di sektor transportasi dan pelayanan kesehatan, IoT terus berkembang pesat, menghadirkan layanan inovatif yang terus ditingkatkan. Dalam beberapa tahun terakhir, terjadi lonjakan drastis dalam adopsi jaringan IoT. Selain meningkatkan keterjangkauan data, jaringan ini juga dihadapkan pada beberapa tantangan yang harus diatasi untuk mencapai operasional yang efisien dan aman. Salah satu keprihatinan utama terkait IoT adalah keamanan. Kurangnya perlindungan yang memadai pada perangkat dan aplikasi IoT dapat berakibat serius, terutama dalam menghadapi potensi serangan siber terhadap fitur yang penting [1].

Serangan siber adalah tindakan kejahatan yang dilakukan oleh individu atau kelompok organisasi, bertujuan merusak atau memperoleh akses ilegal ke dokumen dan sistem kritis dalam jaringan komputer. Baik dalam konteks bisnis maupun pribadi, serangan siber bertujuan menghancurkan atau mengakses informasi rahasia yang dapat memiliki dampak serius [2]. Dari banyaknya serangan siber seperti pada penelitian terkait [3], [4] terdapat berbagai jenis serangan siber yang telah diuraikan dalam penelitian tersebut, salah satunya adalah serangan mirai topik yang akan dijelaskan dalam penelitian ini

Serangan Mirai merupakan serangan DDoS dalam skala besar yang mengincar perangkat IoT. Dengan menginfeksi perangkat, serangan ini membentuk botnet yang dapat membanjiri target dengan lalu lintas yang tinggi. Ancaman ini berpotensi menyebabkan gangguan dalam berbagai konteks. Dengan penyebaran luas perangkat IoT, risiko serangan DDoS juga meningkat, menciptakan kekhawatiran besar terkait keamanan simpul IoT. Dampak dari Mirai tidak hanya mencakup kerugian finansial tetapi juga menekankan perlunya strategi deteksi dan mitigasi yang efektif untuk melawan ancaman ini [3], [5].

Dalam penelitian mengenai deteksi serangan siber, beragam metode digunakan untuk mengidentifikasi dan menganalisis potensi ancaman, seperti penelitian [6] yang menggunakan metode Blockchains, metode ini berbasis Ethereum untuk melindungi IoT dari serangan Mirai. Metode ini melibatkan pembagian jaringan menjadi *Autonomous Systems* (AS) yang saling terkoneksi melalui *blockchain Ethereum*. Setiap AS memiliki tanggung jawab untuk memantau aktivitas host, mengklasifikasikan host sebagai jahat atau normal berdasarkan ambang nilai yang telah ditentukan, dan berbagi daftar node jahat melalui *blockchain*. Walaupun demikian, penelitian ini menyoroti urgensi analisis skalabilitas untuk memahami keterlambatan dalam penyebaran informasi di jaringan, menunjukkan bahwa faktor skalabilitas perlu dipertimbangkan dalam menerapkan metode ini. Dan juga pada penelitian [7] penulis menganalisis paket TCP SYN yang menggunakan tanda tangan Mirai, yaitu dengan nomor urut TCP sama dengan alamat IP tujuan. Tetapi, metode ini tidak mampu membedakan antara paket SYN yang berasal dari Mirai botnet dan paket SYN yang berasal dari protokol TCP konvensional, sehingga berpotensi menghasilkan hasil false positif. Selain itu, metode ini tidak dapat mengukur intensitas serangan mirai botnet secara akurat, karena paket SYN yang dikirim oleh mirai botnet tidak selalu mencerminkan jumlah perangkat yang telah terinfeksi. Selanjutnya pada penelitian [8] menggunakan metode *K-Nearest Neighbors* (KNN), yang merupakan metode pembelajaran mesin yang menggunakan klasifikasi dan regresi, pada dasarnya adalah pendekatan sederhana yang memprediksi kelas atau nilai dari data baru dengan merujuk pada mayoritas kelas atau nilai dari "tetangga terdekat" dalam ruang fitur. Namun, sayangnya, metode ini rentan terhadap *outliers* dan data *noise* karena prediksinya berdasarkan mayoritas "tetangga terdekat” juga pada [9] menggunakan metode *Support Vector Machine* (SVM) merupakan metode yang digunakan untuk pengklasifikasian dan regresi. Fungsi utamanya adalah mencari *hyperplane* optimal yang dapat memisahkan dua kelas dalam ruang fitur. Meskipun demikian, SVM memiliki kelemahan, terutama dalam hal waktu pelatihan yang memakan waktu secara signifikan, dan ketika jumlah sampel atau dimensi fitur sangat besar.

Long Short-Term Memory (LSTM), sebagai jenis arsitektur jaringan saraf tiruan, memberikan kontribusi dalam mendeteksi serangan siber karena kemampuannya dalam pemrosesan urutan data yang efisien dan mengatasi masalah *vanishing gradient* yang umumnya terjadi pada arsitektur jaringan saraf yang lebih sederhana [10]. Kemampuan LSTM tidak hanya terbatas pada retensi informasi dalam jangka waktu yang panjang, tetapi juga dalam kemampuannya untuk menghapus informasi yang tidak berpengaruh secara efektif. Dengan karakteristiknya sebagai jaringan khusus dari jenis RNN, LSTM mampu memahami dependensi dalam jangka panjang [11].

Pada penelitian [12] membandingkan kedua metode *machine learning* yaitu, *Long Short-Term Memory* (LSTM) dan *Support Vector Machine* (SVM) untuk memprediksi kecepatan angin berdasarkan dataset yang diambil dari *kaggle* Temuan dalam penelitian ini menunjukkan bahwa LSTM mengungguli SVM dalam memprediksi kecepatan angin dengan tingkat akurasi yang lebih tinggi. Dibandingkan dengan SVM, LSTM berhasil mengurangi tingkat kesalahan prediksi sekitar 0,005 hingga 0,015. Selain itu, kelebihan LSTM terlihat pada kemampuannya untuk menyesuaikan parameter secara adaptif dan menangkap dengan baik ketergantungan serta perubahan mendadak dalam data kecepatan angin. Dalam penelitian [13], tim peneliti mengajukan sebuah pendekatan terintegrasi yang menggabungkan *Multiscale Convolutional Neural Network* dengan *Long Short Term Memory* (MSCNN-LSTM). Pendekatan ini pertama-tama memanfaatkan *Multiscale Convolutional Neural Network* (MSCNN) untuk menganalisis ciri-ciri spasial dari dataset, dan kemudian menggunakan jaringan *Long Short-Term Memory* (LSTM) untuk memproses ciri-ciri temporal. Dataset yang diuji dalam penelitian ini adalah UNSW NB15. Hasilnya, model MSCNN-LSTM menunjukkan tingkat akurasi yang lebih tinggi, mencapai 89,8%. untuk mendeteksi serangan siber dalam konteks metode manajemen kemacetan berbasis pasar, merupakan fokus penelitian ini [14]. hasil akurasi yang di dapat sebesar 97%. Penelitian pada [15] menggunakan pendekatan deteksi serangan berbasis tanda tangan, sementara modul pertahanan bertujuan untuk mengurangi dampak serangan DDoS yang terdeteksi.

Penelitian [16] di sisi lain, mengulas tentang metode deteksi serangan jaringan yang efektif dengan menerapkan analisis komponen utama berbasis kernel (Kernel PCA) serta jaringan saraf rekuren jangka pendek dan panjang (LSTM-RNN). Tingkat akurasi yang berhasil dicapai mencapai 98,39%. Sementara dalam Penelitian [17], dengan menggunakan dataset CIC DoS yang tersedia untuk umum, peneliti memeriksa efektivitas deteksi dari algoritma deteksi anomali statistik tunggal terhadap serangan DDoS, menghasilkan tingkat akurasi sebesar 88,33%.

Penulis memutuskan untuk mendeteksi Serangan Mirai sebagai fokus penelitian dengan menggunakan metode *Long Short-Term Memory* (LSTM) karena kemampuannya untuk menyimpan informasi yang relevan dalam data yang digunakan. Kelebihan metode LSTM juga terletak pada kemampuannya mengatasi data dengan urutan panjang. Oleh karena itu, penelitian ini memutuskan menggunakan LSTM karena dianggap efektif dalam menghadapi kompleksitas dan karakteristik data yang akan dihadapi, khususnya dalam konteks mendeteksi serangan siber pada CIC IoT 2023.

1.2 Perumusan Masalah

Dalam pelaksanaan Tugas Akhir ini, beberapa permasalahan yang dirumuskan untuk penelitian mencakup :

1. Bagaimana teknik resampling mengatasi menyeimbangkan data yang tidak seimbang dalam sebuah dataset?
2. Bagaimana membangun model *Long Short-Term Memory* (LSTM) dalam mendeteksi serangan mirai pada jaringan IoT?
3. Bagaimana mengukur performa evaluasi accuracy, spesifitas, recall, presisi, dan F1-Score?

1.3 Batasan Masalah

Adapun batasan-batasan yang ditemukan dalam penyusunan tugas akhir ini adalah :

1. Penelitian ini menggunakan teknik undersampling.
2. Penelitian dilakukan pada dataset yang berasal dari *Canadian Institute for Cybersecurity* (CIC) yaitu pada dataset CICIoT 2023.
3. Penelitian ini menghasilkan output berupa beberapa nilai yaitu akurasi, spesifitas, recall, presisi, dan F1-Score sebagai tolak ukur.

1.4 Tujuan

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

1. Menerapkan teknik resampling pada data yang akan diseimbangkan.
2. Membangun model LSTM yang dapat mendeteksi serangan Mirai pada jaringan IoT dengan akurat.
3. Mengevaluasi performa model LSTM dengan menggunakan beberapa metrik evaluasi utama, yaitu akurasi, spesifisitas, recall, presisi, dan F1-Score.

1.5 Manfaat

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

1. Memberikan solusi untuk menyeimbangkan data pada dataset yang tidak seimbang.
2. Memberikan kontribusi pada peningkatan keamanan *cyber*, khususnya dalam konteks IoT.
3. Pengujian performa menggunakan *Long Short-Term Memory* (LSTM) untuk meningkatkan performa dalam pendeteksian serangan mirai.

1.6 Sistematika Penulisan

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

BAB I PENDAHULUAN

Pada bab ini, akan disajikan penjelasan sistematis yang mencakup latar belakang, tujuan, manfaat, perumusan masalah, batasan masalah, dan tata cara penyusunan tugas akhir.

BAB II TINJAUAN PUSTAKA

Bab ini akan merinci teori-teori yang relevan terkait penelitian, khususnya dalam konteks serangan siber.

BAB III METODOLOGI PENELITIAN

Pada bab ini, akan diuraikan langkah-langkah yang dilakukan secara terstruktur, termasuk perancangan sistem dan penerapan metode penelitian.

BAB IV HASIL DAN ANALISA

Dalam bab ini, akan dijelaskan hasil dari pengujian yang telah dilakukan serta analisis data yang dihasilkan dari eksperimen tersebut.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi simpulan serta rekomendasi berdasarkan analisis hasil penelitian yang telah dilakukan.

DAFTAR PUSTAKA

[1] A. Sharma, P. Vibhakar, and M. Kuljeet, “Registered under MSME Government of India Detection of Mirai Botnet Attacks on IoT devices Using Deep Learning,” no. 6, pp. 174–187.

[2] E. Susanto, Lady Antira, K. Kevin, E. Stanzah, and A. A. Majid, “Manajemen Keamanan Cyber Di Era Digital,” *J. Bus. Entrep.*, vol. 11, no. 1, p. 23, 2023, doi: 10.46273/jobe.v11i1.365.

[3] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, “CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment,” *Sensors*, vol. 23, no. 13, 2023, doi: 10.3390/s23135941.

[4] S. Goel and B. Nussbaum, “Attribution across Cyber Attack Types: Network Intrusions and Information Operations,” *IEEE Open J. Commun. Soc.*, vol. 2, no. April, pp. 1082–1093, 2021, doi: 10.1109/OJCOMS.2021.3074591.

[5] T. G. Palla and S. Tayeb, “Intelligent Mirai Malware Detection in IoT Devices,” *2021 IEEE World AI IoT Congr. AIIoT 2021*, pp. 420–426, 2021, doi: 10.1109/AIIoT52608.2021.9454215.

[6] Z. Ahmed, S. M. Danish, H. K. Qureshi, and M. Lestas, “Protecting IoTs from mirai botnet attacks using blockchains,” *IEEE Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD*, vol. 2019-Septe, pp. 1–6, 2019, doi: 10.1109/CAMAD.2019.8858484.

[7] A. Affinito, S. Zinno, G. Stanco, A. Botta, and G. Ventre, “The evolution of Mirai botnet scans over a six-year period,” *J. Inf. Secur. Appl.*, vol. 79, no. October, p. 103629, 2023, doi: 10.1016/j.jisa.2023.103629.

[8] M. A. Lawall, 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, doi: 10.1016/j.procs.2021.02.003.

[9] M. Azizjon, A. Jumabek, and W. Kim, “1D CNN based network intrusion detection with normalization on imbalanced data,” *2020 Int. Conf. Artif. Intell. Inf. Commun. ICAIIC 2020*, pp. 218–224, 2020, doi:

10.1109/ICAIIC48513.2020.9064976.

[10] S. M. Al-Selwi, M. F. Hassan, S. J. Abdulkadir, and A. Muneer, “LSTM Inefficiency in Long-Term Dependencies Regression Problems,” *J. Adv. Res. Appl. Sci. Eng. Technol.*, vol. 30, no. 3, pp. 16–31, 2023, doi: 10.37934/araset.30.3.1631.

[11] 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, no. 18, pp. 26597–26613, 2019, doi: 10.1007/s11042-019-07788-7.

[12] S. Gangwar, V. Bali, and A. Kumar, “o n Scalable Information Systems EAI Endorsed Transactions Comparative Analysis of Wind Speed Forecasting Using LSTM and SVM,” vol. 7, no. 25, pp. 1–9, 2020.

[13] J. Zhang, Y. Ling, X. Fu, X. Yang, G. Xiong, and R. Zhang, “Model of the intrusion detection system based on the integration of spatial-temporal features,” *Comput. Secur.*, vol. 89, p. 101681, Feb. 2020, doi: 10.1016/j.cose.2019.101681.

[14] O. G. M. Khan, A. Youssef, E. El-Saadany, and M. Salama, “LSTM-based approach to detect cyber attacks on market-based congestion management methods,” *IEEE Power Energy Soc. Gen. Meet.*, vol. 2021-July, 2021, doi: 10.1109/PESGM46819.2021.9637976.

[15] H. Aydın, Z. Orman, and M. A. Aydın, “A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment,” *Comput. Secur.*, vol. 118, p. 102725, Jul. 2022, doi: 10.1016/j.cose.2022.102725.

[16] 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.

[17] 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.

[18] F. Ertam, “An efficient hybrid deep learning approach for internet

security," *Phys. A Stat. Mech. its Appl.*, vol. 535, p. 122492, 2019, doi: 10.1016/j.physa.2019.122492.

[19] J. O. Mebawondu, O. D. Alowolodu, J. O. Mebawondu, and A. O. Adetunmbi, "Network intrusion detection system using supervised learning paradigm," *Sci. African*, vol. 9, 2020, doi: 10.1016/j.sciaf.2020.e00497.

[20] A. R. S. Araujo Cruz, R. L. Gomes, and M. P. Fernandez, "An Intelligent Mechanism to Detect Cyberattacks of Mirai Botnet in IoT Networks," in *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, Jul. 2021, pp. 236–243. doi: 10.1109/DCOSS52077.2021.00047.

[21] 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," *Comput. Networks*, vol. 188, no. December 2020, p. 107871, 2021, doi: 10.1016/j.comnet.2021.107871.

[22] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, "A bidirectional LSTM deep learning approach for intrusion detection," *Expert Syst. Appl.*, vol. 185, no. June, p. 115524, 2021, doi: 10.1016/j.eswa.2021.115524.

[23] 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)*, May 2022, pp. 1125–1130. doi: 10.1109/IWCMC55113.2022.9824189.

[24] 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, May 2022, doi: 10.1016/j.asoc.2022.108768.

[25] B. I. Farhan and A. D. Jasim, "Performance analysis of intrusion detection for deep learning model based on CSE-CIC-IDS2018 dataset," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 26, no. 2, p. 1165, May 2022, doi: 10.11591/ijeecs.v26.i2.pp1165-1172.

[26] M. Alshamkhany, W. Alshamkhany, M. Mansour, M. Khan, S. Dhou, and F. Aloul, "Botnet Attack Detection using Machine Learning," *Proc. 2020 14th Int. Conf. Innov. Inf. Technol. IIT 2020*, no. November, pp. 203–208, 2020, doi: 10.1109/IIT50501.2020.9299061.

[27] 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)*, May 2020, pp. 491–497. doi: 10.1109/ICCCS49078.2020.9118459.

[28] N. Oliveira, I. Praça, E. Maia, and O. Sousa, “Intelligent cyber attack detection and classification for network-based intrusion detection systems,” *Appl. Sci.*, vol. 11, no. 4, pp. 1–21, 2021, doi: 10.3390/app11041674.

[29] G. Kambourakis, C. Kolias, and A. Stavrou, “The Mirai botnet and the IoT Zombie Armies,” *Proc. - IEEE Mil. Commun. Conf. MILCOM*, vol. 2017-Octob, pp. 267–272, 2017, doi: 10.1109/MILCOM.2017.8170867.

[30] B. Tushir, H. Sehgal, R. Nair, B. Dezfouli, and Y. Liu, “The Impact of DoS Attacks onResource-constrained IoT Devices:A Study on the Mirai Attack,” 2021, [Online]. Available: http://arxiv.org/abs/2104.09041

[31] A. Rahmatulloh, G. M. Ramadhan, I. Darmawan, N. Widiyasono, and D. Pramesti, “Identification of Mirai Botnet in IoT Environment through Denial-of-Service Attacks for Early Warning System,” *Int. J. Informatics Vis.*, vol. 6, no. 3, pp. 623–628, 2022, doi: 10.30630/joiv.6.3.1262.

[32] 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, Oct. 2020, doi: 10.1016/j.phycom.2020.101157.

[33] R. Mohammed, J. Rawashdeh, and M. Abdullah, “Machine Learning with Oversampling and Undersampling Techniques: Overview Study and Experimental Results,” *2020 11th Int. Conf. Inf. Commun. Syst. ICICS 2020*, pp. 243–248, 2020, doi: 10.1109/ICICS49469.2020.239556.

[34] M. Bach, A. Werner, and M. Palt, “The Proposal of Undersampling Method for Learning from Imbalanced Datasets,” *Procedia Comput. Sci.*, vol. 159, pp. 125–134, 2019, doi: 10.1016/j.procs.2019.09.167.

[35] 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, doi: 10.1109/ACCESS.2020.2985418.

[36] H. Liu and B. Lang, “Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey,” *Appl. Sci.*, vol. 9, no. 20, p. 4396, Oct. 2019, doi: 10.3390/app9204396.

[37] R. C. Staudemeyer and E. R. Morris, “Understanding LSTM -- a tutorial into Long Short-Term Memory Recurrent Neural Networks,” pp. 1–42, 2019, [Online]. Available: http://arxiv.org/abs/1909.09586

[38] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015, doi: 10.1038/nature14539.

[39] Q. Li, F. Wang, J. Wang, and W. Li, “LSTM-based SQL Injection Detection Method for Intelligent Transportation System,” *IEEE Trans. Veh. Technol.*, pp. 1–1, 2019, doi: 10.1109/TVT.2019.2893675.

[40] A. Sahar and D. Han, “An LSTM-based Indoor Positioning Method Using Wi-Fi Signals,” in *Proceedings of the 2nd International Conference on Vision, Image and Signal Processing*, Aug. 2018, pp. 1–5. doi: 10.1145/3271553.3271566.

[41] I. Markoulidakis, G. Kopsiaftis, I. Rallis, and I. Georgoulas, “Multi-Class Confusion Matrix Reduction method and its application on Net Promoter Score classification problem,” *ACM Int. Conf. Proceeding Ser.*, pp. 412–419, 2021, doi: 10.1145/3453892.3461323.