IMPLEMENTASI METODE LSTM-CNN DALAM SISTEM MULTI-CLASSIFICATION DETEKSI SERANGAN SIBER

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana

OLEH :

ADJIE BUDI NEGORO

09011282025096

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

IMPLEMENTASI METODE LSTM-CNN DALAM SISTEM MULTI-CLASSIFICATION DETEKSI SERANGAN SIBER

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar Sarjana

OLEH :

ADJIE BUDI NEGORO

09011282025096

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

HALAMAN PENGESAHAN

IMPLEMENTASI METODE LSTM-CNN DALAM SISTEM MULTI-CLASSIFICATION DETEKSI SERANGAN SIBER

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh :

Adjie Budi Negoro

09011282025096

Palembang, Februari 2024

Mengetahui,

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

AUTHENTICATION PAGE

IMPLEMENTATION OF LSTM-CNN METHOD IN A MULTI-CLASSIFICATION CYBER ATTACK DETECTION SYSTEM

FINAL TASK

Submitted To Fulfill One Of The Requirements To

Obtain A Bachelor's Degree In Computer Science

By :

Adjie Budi Negoro

09011282025096

Palembang, 8/8 Maret 2024

Acknowledge,

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

HALAMAN PERSETUJUAN

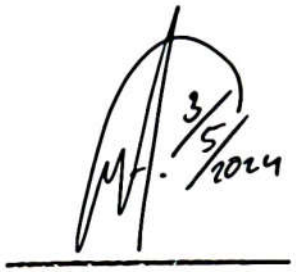
Telah diuji dan lulus pada:

Hari : Kamis

Tanggal : 4 April 2024

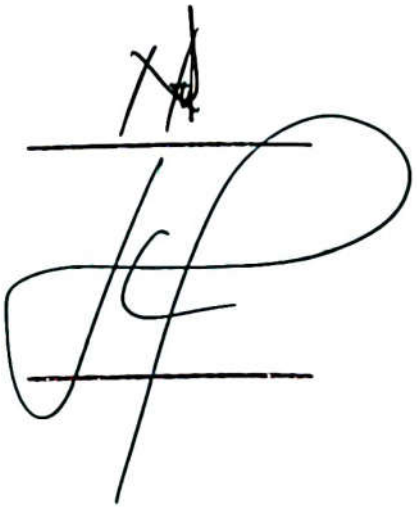
Tim Penguji :

1. **Ketua : Dr. Ahmad Zarkasi, M.T.**



2. **Sekretaris : Nurul Afifah, M.Kom.**

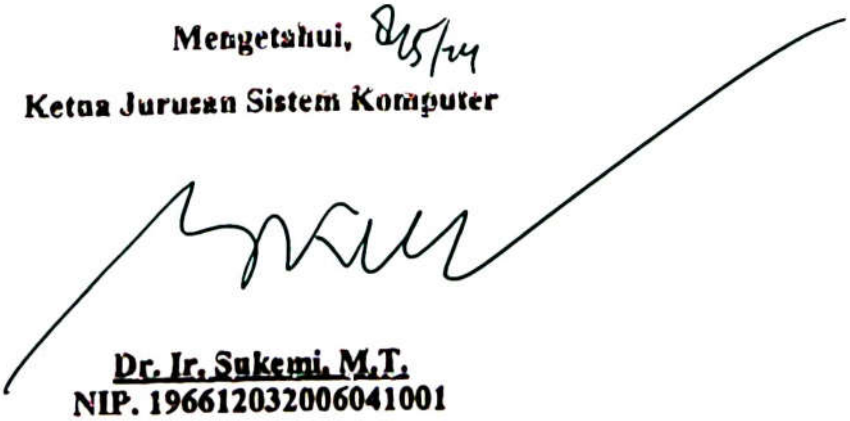
3. **Penguji : Huda Ubaya, M.T.**



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

Mengetahui,

Ketua Jurusan Sistem Komputer



Dr. Jr. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang Bertanda Tangan di Bawah ini:

Nama	:	Adjie Budi Negoro
NIM	:	09011282025096
Judul	:	IMPLEMENTASI METODE LSTM-CNN DALAM SISTEM *MULTI-CLASSIFICATION* DETEKSI SERANGAN SIBER

Hasil Pengecekkam Software iThenticate/Turnitin: 9%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya saya 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, 30 April 2024
Penulis,

Adjie Budi Negoro
NIM.09011282025096

KATA PENGANTAR

Puji dan syukur penulis panjatkan atas kehadirat Allah SWT yang telah memberikan ridho, berkat, dan rahmat-Nya sehingga penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini yang berjudul **"IMPLEMENTASI METODE LSTM-CNN DALAM SISTEM MULTI-CLASSIFICATION DETEKSI SERANGAN SIBER".**

Pada penyusunan laporan ini, saya mengucapkan terima kasih kepada pihak – pihak yang telah memberikan ide dan saran serta bantuan yang diberikan baik secara langsung maupun tidak langsung. Serta memberikan bantuan, dorongan, motivasi, dan bimbingan sehingga saya menjadi lebih semangat. Oleh karena itu, pada kesempatan kali ini penulis mengucapkan rasa syukur kepada Allah SWT yang telah memberikan saya berkat dan rahmat-Nya serta kesehatan yang berlimpah dan terima kasih kepada yang terhormat:

1. Tuhan yesus kristus yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis dalam melaksanakan penelitian ini.
2. Kedua Orang Tua dan Saudara/i saya yang selalu mendoakan, serta memberikan motivasi dan dukungan nya kepada saya,
3. Bapak Prof. Dr. Erwin, S.Si., M.Si selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya,
4. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya,
5. Bapak Ahmad Heryanto, S.Kom,. M.T. selaku Dosen Pembimbing Akademik dan Dosen Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan bimbingan terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini.
6. Kakak tingkat Jurusan Sistem Komputer Universitas Sriwijaya yang telah memberikan bantuan dalam menyelesiakan Tugas Akhir ini,
7. Teman-teman seperjuangan Jurusan Sistem Komputer 2020.
8. Ibu Renny Virgasari selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal-hal administrasi.

9. Dan seluruh pihak yang tidak dapat penulis sebutkan satu per satu, yang selalu memberikan semangat dan bantuan – bantuan yang bermanfaat.

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangatlah diharapkan penulis agar dapat segera diperbaiki sehingga laporan ini dapat dijadikan sebagai masukkan ide dan pemikiran yang bermanfaat bagi semua pihak dan menjadi tambahan bahan bacaan bagi yang tertarik dalam penelitian Network Security.

Akhir kata saya berharap semoga laporan ini dapat bermanfaat serta dapat memberikan pengetahuan dan wawasan bagi semua pihak yang membutuhkannya. Khususnya mahasiswa/i Jurusan Sistem Komputer Universitas Sriwijaya.

Palembang, 30 April 2024

Penulis

Adjie Budi Negoro

NIM. 09011282025096

IMPLEMENTASI METODE LSTM-CNN DALAM SYSTEM MULTI-CLASSIFICATION DETEKSI SERANGAN SIBER

Adjie Budi Negoro (09011282025096)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: adjie544@gmail.com

ABSTRAK

Serangan Siber adalah upaya yang dilakukan oleh individu atau kelompok untuk menyerang sistem komputer, jaringan, atau perangkat elektronik lainnya dengan maksud mencuri data sensitif, merusak infrastruktur, atau menciptakan gangguan dalam layanan. Ada berbagai jenis serangan siber, termasuk serangan malware, serangan phishing, serangan DDoS (Distributed Denial of Service), serangan ransomware, dan banyak lagi. Cara yang dilakukan untuk melindungi sistem keamanan jaringan terhadap macam-macam serangan siber, 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 Long Short Term Memory – Convolutional Neural Network (LSTM-CNN). Penelitian ini menggunakan empat dataset yang berbeda-beda yaitu KDD-Cup99, NSL-KDD, ISCX 2012, dan CIC-IDS 2018 dengan berbagai macam serangan yang ada didalamnya. Dengan melakukan validasi pada data training dan testing dari 20% sampai 80%. Sebagai output dari penelitian ini menghasilkan performa nilai yang terbaik berupa Akurasi untuk dataset KDD-Cup99 sebesar 99,96%, Recall 99,96%, Spesifitas 99.99%, Presisi 99,96%, F1-Score 99,96%. Akurasi untuk dataset NSL-KDD sebesar 99,78%, Recall 99,78%, Spesifitas 99.94%, Presisi 99,78%, F1-Score 99,77%. Akurasi untuk dataset ISCX 2012 sebesar 99,58%, Recall 99,58%, Spesifitas 99.92%, Presisi 99,58%, F1-Score 99,58%. Akurasi untuk dataset CIC-IDS 2018 sebesar 99.95%, Recall 99.95%, Spesifitas 100.00%, Presisi 99.95%, F1-Score 99.95%.

Kata kunci: *Serangan Siber, Intrusion Detection System, Dataset KDD-Cup99, Dataset NSL-KDD, Dataset ISCX 2012, Dataset CIC-IDS 2018, Long Short-Term Memory, Convolutional Neural Network.*

Mengetahui,

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

IMPLEMENTATION OF LSTM-CNN METHOD IN A MULTI-CLASSIFICATION SYSTEM FOR CYBER ATTACK DETECTION

Adjie Budi Negoro (09011282025096)
Department of Computer Systems, Faculty of Computer Science, Sriwijaya University
Email: adjie544@gmail.com

ABSTRACT

Cyberattacks are attempts by individuals or groups to attack computer systems, networks, or other electronic devices with the intent of stealing sensitive data, damaging infrastructure, or creating disruptions in service. There are various types of cyber-attacks, including malware attacks, phishing attacks, DDoS (Distributed Denial of Service) attacks, ransomware attacks, and more. To protect the network security system against various types of cyber-attacks, an attack detection system such as an Intrusion Detection System is needed. IDS is a detector that can investigate activities that occur on internet systems and networks. The method used in this research is Long Short-Term Memory – Convolutional Neural Network (LSTM-CNN). This research uses four different datasets, namely KDD-Cup99, NSL-KDD, ISCX 2012, and CIC-IDS 2018 with various types of attacks in them. By validating training and testing data from 20% to 80%. The output of this research produces the best performance values in the form of Accuracy for the KDD-Cup99 dataset of 99.96%, Recall 99.96%, Specificity 99.99%, Precision 99.96%, F1-Score 99.96%. Accuracy for the NSL-KDD dataset is 99.78%, Recall 99.78%, Specificity 99.94%, Precision 99.78%, F1-Score 99.77%. Accuracy for the ISCX 2012 dataset is 99.58%, Recall 99.58%, Specificity 99.92%, Precision 99.58%, F1-Score 99.58%. Accuracy for the 2018 CIC-IDS dataset is 99.95%, Recall 99.95%, Specificity 100.00%, Precision 99.95%, F1-Score 99.95%.

Keywords: *Cyber Attack, Intrusion Detection System, KDD-Cup99 Dataset, NSL-KDD Dataset, ISCX 2012 Dataset, CIC-IDS 2018 Dataset, Long Short-Term Memory, Convolutional Neural Network.*

Acknowledge,

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

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era yang semakin terhubung secara digital, keamanan informasi dan infrastruktur teknologi informasi menjadi hal yang semakin krusial. Serangan cyberattack telah menjadi ancaman serius yang dapat mengganggu stabilitas dan integritas sistem di seluruh dunia [1]. Untuk mengatasi ancaman ini, langkah-langkah efektif dalam mendeteksi serangan sebelum terjadi menjadi sangat penting, sehingga dapat meminimalkan dampak yang mungkin timbul jika serangan tersebut berhasil [2].

Dalam upaya mendeteksi serangan siber, berbagai teknik deteksi telah dikembangkan, termasuk di antaranya adalah menggunakan metode jaringan saraf [3]. Salah satu teknik yang banyak digunakan adalah multi-class classification, yang memungkinkan pengkategorian data uji menjadi beberapa label kelas yang telah ditentukan sesuai dengan data latihan [4]. Hal ini memungkinkan untuk mengidentifikasi berbagai jenis serangan secara bersamaan, meningkatkan efisiensi dalam respons terhadap ancaman cyber.

Dalam konteks keamanan cyber, metode LSTM-CNN telah menjadi populer karena kemampuannya dalam memproses data urutan dan pengenalan pola yang kompleks [5]. LSTM, yang merupakan modifikasi dari Recurrent Neural Network (RNN), efektif dalam memahami konteks temporal dari data sekuensial [5]. Sementara CNN, yang merupakan bagian dari deep neural network, dapat mengekstraksi fitur spasial dari data, terutama data visual seperti citra dan piksel [6] [7].

Studi-studi sebelumnya telah menunjukkan keberhasilan metode LSTM-CNN dalam mendeteksi aktivitas manusia dan serangan siber dengan tingkat akurasi yang memuaskan [8] [9] [10]. Gabungan LSTM-CNN memungkinkan model untuk menangkap fitur spasial dan sekuensial yang berkaitan dengan serangan siber, sehingga meningkatkan kemampuan dalam mengenali pola kompleks dalam data sekuensial dan spasial [6].

Dengan demikian, implementasi metode LSTM-CNN dalam sistem multi-classification deteksi serangan siber menjadi langkah yang penting untuk meningkatkan akurasi dan keberlanjutan model, serta memungkinkannya untuk merespons serangan dengan lebih efektif dan efisien. Dengan kemampuan untuk menangkap fitur-fitur penting dari data, metode ini diharapkan dapat menjadi solusi yang lebih baik dalam menghadapi ancaman cyber yang terus berkembang.

1.2 Perumusan Masalah

Dari latar belakang diatas permasalahan yang akan dibahas pada penelitian ini agar mengerucut dan tidak melebar pada permasalahan lain ialah :

1. Seberapa efektif penggunaan multi-classification dengan metode LSTM-CNN dalam mendeteksi dan membandingkan berbagai jenis serangan siber yang beraneka ragam?
2. Dengan data yang sangat besar dan beragamnya jenis serangan siber, bagaimana teknik yang dapat diadopsi untuk mengelola data tersebut secara efisien? Selain itu, bagaimana meningkatkan akurasi dan kecepatan komputasi dalam proses deteksi serangan siber?

1.3 Tujuan Penulisan

Berdasarkan latar belakang diatas maka didapat tujuan dari penelitian ini sebagai berikut:

1. Meneliti dan menganalisis metode LSTM-CNN dalam sistem *multi-classification* untuk deteksi *cyberattack.*
2. Mengevaluasi kinerja dan akurasi deteksi *cyberattack* yang dilakukan oleh metode LSTM-CNN dalam sistem *multi-classification*, dan membandingkannya dengan teknik deteksi *cyberattack* lainnya.

1.4 Manfaat Penulisan

Berdasarkan tujuan yang ingin dicapai maka didapat manfaat dari penelitian ini yang diharapkan dapat memberikan manfaat sebagai berikut:

1. Meningkatkan pemahaman tentang teknologi deteksi *cyberattack*, serta berbagai teknik yang digunakan untuk mendeteksi serangan tersebut.

2. Mengetahui kemampuan dan keterbatasan metode LSTM-CNN dalam sistem *multi-classification* untuk deteksi *cyberattack*.
3. Mengetahui bagaimana cara mengimplementasikan metode LSTM-CNN dalam sistem *multi-classification* untuk deteksi *cyberattack*, serta teknologi dan bahasa pemrograman yang relevan.
4. Memiliki pengetahuan tentang bagaimana cara meningkatkan kinerja dan akurasi deteksi *cyberattack* dengan metode LSTM-CNN dalam sistem *multi-classification*.
5. Memberikan kontribusi bagi pengembangan teknologi keamanan jaringan komputer, yang dapat membantu meningkatkan keamanan sistem informasi dan mencegah kerugian akibat *cyberattack*.

1.5 Batasan Masalah

Batasan masalah yang didapatkan pada penelitian tugas akhir ini antara lain :

1. Berfokus pada pendeteksian *cyberattack* pada jaringan komputer menggunakan Long short-term memory methods (LSTM) dan Convolutional neural network (CNN) dalam sistem deteksi multi-klasifikasi.
2. Dataset yang dipakai dalam penelitian kali ini adalah KDD-CUP99, NSL-KDD, CIC-IDS 2018, ISCX 2012.
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,

1.6 Sistematika Penelitian

Penelitian yang digunakan oleh peneliti pada tugas akhir ini, antara lain:

BAB I PENDAHULUAN

Pada bab bagian pertama berisikan paparan secara sistematis latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab tugas akhir bagian kedua berisikan penjelasan teori dasar yang menunjang penelitian ini. Dasar teori tersebut membahas literatur terhadap membahas konsep dasar dari metode LSTM-CNN, teknik-teknik pre-processing data, teknik augmentasi data, teknik ensemble learning, dan teknik evaluasi model LSTM dan CNN.

BAB III METODOLOGI PENELITIAN

Pada bab penelitian bagian ketiga ini menjelaskan bagaimana proses saat menjalankan penelitian, dimulai dari tahap persiapan data, pengolahan data, ekstraksi fitur, pembagian data latih dan uji dengan beberapa Hyperparameter dan validasi performa.

BAB IV HASIL DAN PEMBAHASAN

Pada bab bagian empat pada penelitian ini menjelaskan perolehan hasil dan analisa akhir dari penelitian yang telah dilakukan sebelumnya oleh peneliti.

BAB V KESIMPULAN

Pada bab yang kelima ini merupakan bagian kesimpulan berdasarkan perolehan dari hasil dan analisa pada evaluasi pengujian terhadap penelitian telah selesai dilakukan.

DAFTAR PUSTAKA

[1] S. Lauder Siagian, Arief Budiarto2, "THE ROLE OF CYBER SECURITY IN OVERCOME NEGATIVE CONTENTS TO REALIZE NATIONAL INFORMATION RESILIENCE," 2018.

[2] A. Vivi Kumalasari S., S.E, M.Si, *Dalam Bidang Teknologi Informasi*. 2008.

[3] M. A. Ridho and M. Arman, "Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 3, pp. 373–379, Oct. 2020, doi: 10.32736/sisfokom.v9i3.945.

[4] A. I. S. Azis, P. Pascasarjana, M. T. Informatika, and U. D. Nuswantoro, "Model Multi Clas Svm Menggunakan Strategi 1V1 Untuk Klasifikasi Wall-Following Robot Navigation Data Model Multi Clas Svm Menggunakan Strategi 1V1 Untuk Klasifikasi Wall-Following Robot Navigation Data," 2013.

[5] D. T. Hermanto, A. Setyanto, and E. T. Luthfi, "Algoritma LSTM-CNN untuk Binary Klasifikasi dengan Word2vec pada Media Online," *Creat. Inf. Technol. J.*, vol. 8, no. 1, p. 64, Mar. 2021, doi: 10.24076/citec.2021v8i1.264.

[6] A. Saaudi, Z. Al-Ibadi, Y. Tong, and C. Farkas, "Insider threats detection using CNN-LSTM model," in *Proceedings - 2018 International Conference on Computational Science and Computational Intelligence, CSCI 2018*, Dec. 2018, pp. 94–99. doi: 10.1109/CSCI46756.2018.00025.

[7] A. A. Kurniawan and M. Mustikasari, "Implementasi Deep Learning Menggunakan Metode CNN dan LSTM untuk Menentukan Berita Palsu dalam Bahasa Indonesia," *J. Inform. Univ. Pamulang*, vol. 5, no. 4, p. 544, 2021, doi: 10.32493/informatika.v5i4.6760.

[8] K. Xia, J. Huang, and H. Wang, "LSTM-CNN Architecture for Human Activity Recognition," *IEEE Access*, vol. 8, pp. 56855–56866, 2020, doi: 10.1109/ACCESS.2020.2982225.

[9] Q. H. Vo, H. T. Nguyen, B. Le, and M. Le Nguyen, "Multi-channel LSTM-CNN model for Vietnamese sentiment analysis," in *Proceedings - 2017 9th International Conference on Knowledge and Systems Engineering, KSE 2017*, 2017, vol. 2017-Janua, pp. 24–29. doi: 10.1109/KSE.2017.8119429.

[10] P. Nagabushanam, S. Thomas George, and S. Radha, "EEG signal classification using LSTM and improved neural network algorithms," *Soft Comput.*, vol. 24, no. 13, pp. 9981–10003, 2020, doi: 10.1007/s00500-019-04515-0.

[11] M. S. Pervez and D. M. Farid, "Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs," in *The 8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2014)*, Dec. 2014, pp. 1–6. doi: 10.1109/SKIMA.2014.7083539.

[12] 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.

[13] K. N. Junejo and J. Goh, "Behaviour-based attack detection and classification in cyber physical systems using machine learning," *CPSS 2016 - Proc. 2nd ACM Int. Work. Cyber-Physical Syst. Secur. Co-located with Asia CCS 2016*, no. Ml, pp. 34–43, 2016, doi: 10.1145/2899015.2899016.

[14] 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.

[15] 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.

[16] S. N. Nguyen, V. Q. Nguyen, J. Choi, and K. Kim, “Design and implementation of intrusion detection system using convolutional neural network for DoS detection,” *ACM Int. Conf. Proceeding Ser.*, pp. 34–38, 2018, doi: 10.1145/3184066.3184089.

[17] L. Zhou, X. Ouyang, H. Ying, L. Han, Y. Cheng, and T. Zhang, “Cyber-attack classification in smart grid via deep neural network,” *ACM Int. Conf. Proceeding Ser.*, pp. 1–5, 2018, doi: 10.1145/3207677.3278054.

[18] 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.

[19] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble, “Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data,” *IEEE Trans. Ind. Informatics*, vol. 15, no. 7, pp. 4362–4369, 2019, doi: 10.1109/TII.2019.2891261.

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

[21] J. Zhang, “DeepMal: A CNN-LSTM model for malware detection based on dynamic semantic behaviours,” in *Proceedings - 2020 International Conference on Computer Information and Big Data Applications, CIBDA 2020*, Apr. 2020, pp. 313–316. doi: 10.1109/CIBDA50819.2020.00077.

[22] A. Mishra, A. M. K. Cheng, and Y. Zhang, “Intrusion Detection Using Principal Component Analysis and Support Vector Machines,” in *IEEE International Conference on Control and Automation, ICCA*, Oct. 2020, vol. 2020-Octob, pp. 907–912. doi: 10.1109/ICCA51439.2020.9264568.

[23] H. Alqahtani, I. H. Sarker, A. Kalim, S. M. Minhaz Hossain, S. Ikhlaq, and S. Hossain, *Cyber intrusion detection using machine learning classification techniques*, vol. 1235 CCIS. Springer Singapore, 2020. doi: 10.1007/978-

981-15-6648-6_10.

[24] Q. A. Al-Haija and S. Zein-Sabatto, “An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks,” *Electron.*, vol. 9, no. 12, pp. 1–26, 2020, doi: 10.3390/electronics9122152.

[25] 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.

[26] 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.

[27] 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.

[28] P. Ganesh *et al.*, “Learning-Based Simultaneous Detection and Characterization of Time Delay Attack in Cyber-Physical Systems,” *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3581–3593, 2021, doi: 10.1109/TSG.2021.3058682.

[29] M. Khonji, Y. Iraqi, and A. Jones, “Phishing detection: A literature survey,” *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4. pp. 2091–2121, 2013. doi: 10.1109/SURV.2013.032213.00009.

[30] A. Qamar, A. Karim, and V. Chang, “Mobile malware attacks: Review, taxonomy & future directions,” *Futur. Gener. Comput. Syst.*, vol. 97, pp. 887–909, Aug. 2019, doi: 10.1016/j.future.2019.03.007.

[31] E. M. Rudd, A. Rozsa, M. Günther, and T. E. Boult, “A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions,” *IEEE Communications Surveys and Tutorials*, vol. 19, no. 2. Institute of Electrical and Electronics Engineers Inc., pp. 1145–

1172, Apr. 01, 2017. doi: 10.1109/COMST.2016.2636078.

[32] Z. Čekerevac, Z. Dvorak, L. Prigoda, and P. Čekerevac, “INTERNET OF THINGS AND THE MAN-IN-THE-MIDDLE ATTACKS – SECURITY AND ECONOMIC RISKS,” *MEST J.*, vol. 5, no. 2, pp. 15–5, Jul. 2017, doi: 10.12709/mest.05.05.02.03.

[33] J. Komputer, G. Ngurah, A. Sucipta, I. Made, W. Wirawan, and A. Muliantara, “ANALISIS KINERJA ANOMALY-BASED INTRUSION DETECTION SYSTEM (IDS) DALAM MENDETEKSI SERANGAN DOS (DENIAL OF SERVICES) PADA,” 2012.

[34] F. Salahdine and N. Kaabouch, “Social engineering attacks: A survey,” *Future Internet*, vol. 11, no. 4. Multidisciplinary Digital Publishing Institute, p. 89, Apr. 02, 2019. doi: 10.3390/FI11040089.

[35] R. Kalniņš, J. Puriņš, and G. Alksnis, “Security Evaluation of Wireless Network Access Points,” *Appl. Comput. Syst.*, vol. 21, no. 1, pp. 38–45, May 2017, doi: 10.1515/ACSS-2017-0005.

[36] G. Huafeng, X. Changcheng, and C. Shiqiang, “Wearable sensors for human activity recognition based on a self-attention CNN-BiLSTM model,” *Sens. Rev.*, no. July, 2023, doi: 10.1108/SR-10-2022-0398.

[37] W. Wang, X. Du, D. Shan, R. Qin, and N. Wang, “Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine,” *IEEE Trans. Cloud Comput.*, vol. 10, no. 3, pp. 1634–1646, 2022, doi: 10.1109/TCC.2020.3001017.

[38] D. Setiawan, A. Dwi Putra, K. Stefani, and J. Felisa, “Implementasi Convolutional Neural Network untuk Facial Recognition,” *Media Inform.*, vol. 20, no. 2, pp. 66–79, Jul. 2021, doi: 10.37595/mediainfo.v20i2.68.

[39] M. Gohil and S. Kumar, “Evaluation of Classification algorithms for Distributed Denial of Service Attack Detection,” in *Proceedings - 2020 IEEE 3rd International Conference on Artificial Intelligence and Knowledge Engineering, AIKE 2020*, Dec. 2020, pp. 138–141. doi:

10.1109/AIKE48582.2020.00028.

[40] D. I. AF'IDAH, R. Kusumaningrum, and B. Surarso, *LONG SHORT TERM MEMORY-CONVOLUTIONAL NEURAL NETWORK PADA ANALISIS SENTIMEN ULASAN OBJEK WISATA DI PULAU BALI BERBAHASA ….* 2020. Accessed: Mar. 09, 2023. [Online]. Available: https://eprints2.undip.ac.id/id/eprint/5879/%0Ahttps://eprints2.undip.ac.id/id/eprint/5879/3/FINAL TESIS_DWI INTAN A bab 2 -pages-19-40.pdf

[41] Y. Yohannes, Y. P. Sari, and I. Feristyani, "Klasifikasi Wajah Hewan Mamalia Tampak Depan Menggunakan k-Nearest Neighbor Dengan Ekstraksi Fitur HOG," *J. Tek. Inform. dan Sist. Inf.*, vol. 5, no. 1, May 2019, doi: 10.28932/jutisi.v5i1.1584.

[42] N. Rachmat, Y. Yohannes, and A. Mahendra, "Klasifikasi Jenis Ikan Laut Menggunakan Metode SVM dengan Fitur HOG dan HSV," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 4, pp. 2235–2247, Dec. 2021, doi: 10.35957/jatisi.v8i4.1686.

[43] Dwi Widiastuti, "ANALISA PERBANDINGAN ALGORITMA SVM, NAIVE BAYES, DAN DECISION TREE DALAM MENGKLASIFIKASIKAN SERANGAN (ATTACKS) PADA SISTEM PENDETEKSI INTRUSI".