SISTEM DETEKSI *MULTI-CLASSIFICATION* SERANGAN *CYBER* MENGGUNAKAN METODE *DEEP LEARNING CNN*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :
SARI NURHALIZA
09011282025040

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2024

HALAMAN PENGESAHAN

SISTEM DETEKSI *MULTI-CLASSIFICATION* SERANGAN *CYBER* MENGGUNAKAN METODE *DEEP LEARNING CNN*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

SARI NURHALIZA

09011282025040

Indralaya, 4 April 2024

Mengetahui,

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

AUTHENTICATION PAGE

MULTI CLASSIFICATION DETECTION SYSTEM CYBER ATTACKS USING METHODS CNN DEEP LEARNING

SKRIPSI

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

By :

SARI NURHALIZA

09011282025040

Indralaya, 4 April 2024

Acknowledge,

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Jumat

Tanggal : 22 Maret 2024

Tim Penguji:

1. Ketua : Dr. Rossi Passarella, M. Eng.
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. Ir Sukemi, M. T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang Bertanda Tangan Di Bawah Ini :

Nama	:	Sari Nurhaliza
NIM	:	09011282025040
Judul	:	SISTEM DETEKSI *MULTI-CLASSIFICATION* SERANGAN *CYBER* MENGGUNAKAN METODE *DEEP LEARNING CNN*

Hasil Pengecekkam Software iThenticate/Turnitin : 5%

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, 4 April 2024
Penulis,

Sari Nurhaliza
NIM.09011282025040

KATA PENGANTAR

Puji Syukur penulis panjatkan kehadirat Allah swt. atas limpahan rahmat dan karunianya, sehingga penulis dapat menyelesaikan penyusunan Laporan Tugas Akhir ini yang berjudul **"Sistem Deteksi Multi-Classification Serangan Cyber Menggunakan Metode Deep Learning Cnn"**.

Penyusunan Laporan Tugas Akhir ini tidak terlepas dari peran serta beberapa pihak yang turut membantu oleh karena itu dengan hati yang tulus dan penuh keihklasan, penulis ingin menyampaikan rasa syukur dan terimakasih serta penghargaan yang tak terhingga sedalam-dalamnya kepada:

1 Allah SWT. yang telah memberikan kesehatan, kemudahan, serta keberkahan sehingga penulis dapat menyelesaikan kerja praktik beserta laporannya dengan baik.

2 Orang tua penulis yang telah membesarkan saya dengan penuh kasih sayang dan telah banyak memberikan do'a serta dukungan dan semangat kepada penulis dalam menyelesaikan pengerjaan Tugas Akhir.

3 Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya dan selaku Dosen Pembimbing Akademik yang telah berkenan memberikan saran dan arahan untuk penulis dalam menyiapkan Tugas Akhir.

4 Bapak Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan tugas akhir ini.

5 Mbak Renny dan Pak Yopi selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.

6 Kepada teman seperjuangan penulis saudari Titin Agistina, Maratus Sholikah, Cikal Khairrun Nissa, dan Khairunnisya yang menjadi teman selama perkuliahan.

7 Kepada teman-teman kelas SKB 2020 dan teman teman di Lab Comnets.

8 Kepada rekan seperjuangan Riset Grup MC yang telah menjadi teman dalam mengejar akurasi.

9 Kepada anggota Group EXO terkhususnya Kim Jongin yang telah memberikan dukungan kepada penulis secara tidak langsung melalui karya-karyanya.

10 Last but not least, I wanna thank me I wanna thank me for believing in me, I wanna thank me for doing all this hard work, I wanna thank me for having no days off, I wanna thank me for never quitting, I wanna thank me for always being a giver and tryna give more than I receive, I wanna thank me for tryna do more right than wrong, I wanna thank me for just being me at all times.

11 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. Akhir kata penulis berharap, semoga proposal tugas akhir ini bermanfaat dan berguna bagi khalayak.

Indralaya, 4 April 2024

Penulis,

Sari Nurhaliza

NIM. 09011282025040

SISTEM DETEKSI MULTI-CLASSIFICATION SERANGAN CYBER MENGGUNAKAN METODE DEEP LEARNING CNN

SARI NURHALIZA
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : sarinrhlz00@gmail.com

ABSTRAK

Serangan cyber telah menjadi ancaman yang semakin meningkat terhadap keamanan sistem informasi modern. Untuk mengatasi kompleksitas dan keberagaman serangan yang terjadi, pendekatan deteksi yang canggih dan andal sangat diperlukan. Dalam penelitian ini, kami mengusulkan sebuah sistem deteksi multi-classification serangan cyber yang mengadopsi metode Deep Learning Convolutional Neural Network (CNN). CNN telah terbukti efektif dalam mengatasi masalah klasifikasi gambar dan telah menunjukkan potensi besar dalam aplikasi deteksi serangan cyber. Kami mengumpulkan dataset yang representatif dari berbagai jenis serangan cyber dan melatih model CNN untuk mengidentifikasi serangan dalam kategori multi-classification. Eksperimen dilakukan untuk mengevaluasi kinerja sistem deteksi yang diusulkan, termasuk pengujian terhadap kecepatan deteksi dan tingkat akurasi. Hasil menunjukkan bahwa sistem yang diusulkan mampu mendeteksi serangan cyber dengan tingkat akurasi yang tinggi, sementara juga mempertahankan kecepatan deteksi yang memadai. Kontribusi utama dari penelitian ini adalah pengembangan sistem deteksi yang dapat memberikan perlindungan yang efektif terhadap serangan cyber yang beragam, dengan memanfaatkan kekuatan metode Deep Learning CNN.

kata kunci : Serangan cyber, Deteksi serangan, Deep Learning, Convolutional Neural Network, Multiclassification.

Mengetahui,

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

MULTI CLASSIFICATION DETECTION SYSTEM CYBER ATTACKS USING METHODS CNN DEEP LEARNING

SARI NURHALIZA
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : sarinrhlz00@gmail.com

ABSTRACT

Cyber attacks have become an increasing threat to the security of modern information systems. To overcome the complexity and diversity of attacks that occur, a sophisticated and reliable detection approach is needed. In this research, we propose a multi-classification cyber attack detection system that adopts the Deep Learning Convolutional Neural Network (CNN) method. CNNs have proven effective in solving image classification problems and have shown great potential in cyber attack detection applications. We collect a representative dataset of various types of cyber attacks and train a CNN model to identify attacks in multi-classification categories. Experiments were carried out to evaluate the performance of the proposed detection system, including testing the detection speed and accuracy level. The results show that the proposed system is capable of detecting cyber attacks with a high degree of accuracy, while also maintaining sufficient detection speed. The main contribution of this research is the development of a detection system that can provide effective protection against various cyber attacks, by exploiting the power of the Deep Learning CNN method.

Keywords : Cyber attacks, Attack detection, Deep Learning, Convolutional Neural Network, Multiclassification.

Acknowledge,

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

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Serangan *cyber* merupakan tindakan agresi yang dilakukan melalui penggunaan jaringan komputer dengan tujuan membahayakan target serangan. Serangan *cyber* dapat terjadi dalam berbagai bentuk, termasuk pencurian data, gangguan sistem komputer, dan penghancuran infrastruktur penting[1]. Serangan *cyber* melibatkan tindakan dan operasi yang disengaja untuk mengubah, mengganggu, menipu, menurunkan, atau menghancurkan sistem atau jaringan komputer musuh, serta informasi dan program yang ada di dalam atau ditransmisikan melalui sistem atau jaringan tersebut. Serangan *cyber* bersifat merusak dan dapat mencakup penghapusan oleh virus komputer yang menetap di *hard disk* komputer mana pun yang terinfeksi[2].

Pada tahun 2022, tercatat kerusakan akibat serangan *cyber* mencapai 2 triliun, jumlah yang signifikan hingga saat ini. Serangan *cyber* terjadi setiap 39 detik, menurut data yang ada. Para analis memprediksi bahwa Amerika Serikat akan menjadi target lebih dari 50% serangan *cybercrime* di seluruh dunia dalam lima tahun mendatang[3]. Dalam periode 12 bulan terakhir, sebanyak 66% bisnis telah mengalami serangan *cyber*, dengan 43% dari serangan tersebut ditujukan kepada bisnis kecil. Sayangnya, hanya 14% bisnis yang memiliki kesiapan dalam membela diri terhadap serangan-serangan tersebut. Selain itu, serangan *cyber* pada perangkat *Internet of Things* (IoT) diperkirakan akan meningkat dua kali lipat pada tahun 2025[4].

Penelitian oleh CSO menunjukkan bahwa biaya kerusakan akibat *cybercrime* telah melampaui 6 triliun dolar per tahun pada tahun 2021, dengan waktu rata-rata untuk mendeteksi intrusi meningkat dari 57,4 hari menjadi 93,2 hari dalam tiga tahun terakhir[5]. Dalam sepuluh tahun terakhir, serangan *cyber* memicu kerusakan yang tidak dapat diperbaiki pada masyarakat kita. Pada 2013, berbagai kelompok peretas

menyusup ke 1 miliar akun Yahoo. Pada 2014, ada 145 juta pengguna eBay di bawah serangan *cyber*. Pada 2017, instruksi *cyber* mendapatkan 143 juta informasi pribadi konsumen dari Equifax2[6] .

Pada jurnal penelitian " *A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments* ", journal ini memberikan gambaran luas tentang kemajuan standar yang disajikan di bidang keamanan *cyber* dan menyelidiki tantangannya. Namun, penelitian tersebut tidak memberikan analisis komprehensif tentang kelemahan klasifikasi serangan *cyber*, dan tidak memberikan metodologi yang jelas tentang bagaimana kemajuan standar disurvei dan ditinjau secara komprehensif atau kriteria yang digunakan untuk menyelidiki tantangan[7].

Dalam penelitian ini, penulis menggunakan metode CNN. *Convolutional neural networks* (CNN) adalah *feed-forward neural networks* yang menjadi populer dalam pemrosesan gambar setelah karya terobosan LeCunn et al[8]. CNN secara signifikan meningkatkan efisiensi jaringan saraf dengan menerapkan konvolusi, yang pada dasarnya adalah sebuah filter, ke area input yang lebih kecil daripada melakukan perkalian matriks pada seluruh gambar secara bersamaan[9]. Sementara CNN tradisional digunakan dalam pemrosesan gambar yang bersifat 2D, CNN 1D dapat digunakan dengan berhasil dalam pemrosesan deret waktu. Hal ini dikarenakan deret waktu memiliki lokalitas 1D (waktu) yang kuat yang dapat diekstraksi secara efektif melalui konvolusi[10]. Algoritma *deep learning* bertujuan untuk mempelajari pola dari dataset dalam jumlah besar[6]. Dalam pekerjaan ini kami menunjukkan bahwa Metode CNN yang digunakan pada sistem ini mampu memproses data dalam jumlah besar dan kompleks dengan lebih efektif dibandingkan metode klasik.

Dataset-dataset yang digunakan merupakan sebuah data set yang berisi informasi mengenai serangan *cyber*. Data set ini memuat informasi mengenai lalu lintas jaringan internet, jenis-jenis serangan *cyber*, dan beberapa atribut lainnya yang relevan dalam deteksi serangan *cyber*. Pada sistem deteksi multi-classification serangan *cyber* menggunakan metode *deep learning* CNN dengan dataset-dataset yang digunakan seperti Kdd-Cup99, Iscx2012, Nsl-Kdd, dan CICDdos 2019, data set tersebut digunakan sebagai data latih (training data) untuk melatih model CNN

sehingga dapat melakukan klasifikasi serangan *cyber* dengan akurasi yang tinggi. Setelah model CNN dilatih dengan data set, model tersebut kemudian dapat diuji pada data yang belum pernah dilihat sebelumnya (testing data) untuk mengetahui akurasi dari model.

Hasil penelitian menunjukkan bahwa sistem deteksi multi-classification serangan *cyber* menggunakan metode *deep learning* CNN dengan dataset yang digunakan dapat mengklasifikasikan serangan dengan akurasi yang tinggi. Dengan adanya sistem deteksi ini, diharapkan dapat membantu organisasi dalam mendeteksi serangan *cyber* dan mengambil tindakan yang tepat untuk melindungi jaringan mereka. Berdasarkan latar belakang yang telah di bahas, Penelitian ini akan membahas tentang deteksi *multi-classification* serangan *cyber* yang diberi judul **"sistem deteksi multi-classification serangan *cyber* menggunakan metode *deep learning* CNN"**

1.2 Tujuan

Berdasarkan latar belakang yang telah dikemukakan di atas, maka penulis dapat memberitahukan tujuan dari penulisan Tugas Akhir ini yaitu:

1. mengoptimalkan sistem deteksi serangan *cyber multi-classification* agar mampu mengklasifikasikan lalu lintas jaringan dengan akurasi tinggi sebagai normal atau berbahaya.
2. meningkatkan efektivitas sistem deteksi serangan *cyber* multi-kelas dengan tujuan dapat mengklasifikasikan lalu lintas jaringan secara akurat sebagai normal atau berbahaya dengan tingkat akurasi yang tinggi.
3. mengembangkan kerangka kerja yang efektif untuk membangun sistem deteksi serangan *cyber* menggunakan metode *deep learning Convolutional Neural Network* (CNN).
4. Mampu mengembangkan sistem deteksi serangan *cyber multi-classification* menggunakan metode *deep learning* CNN

1.3 Manfaat

Adapun manfaat dari penulisan Tugas Akhir ini, yaitu:

1. Pemanfaatan deep learning dalam mendeteksi serangan cyber dengan multi-kelas dapat secara signifikan meningkatkan akurasi dan efisiensi sistem deteksi intrusi
2. Dapat mempelajari pola kompleks dari data sehingga dapat sangat efektif dalam mendeteksi serangan cyber yang sering kali memiliki pola perilaku rumit dan tidak selalu terlihat jelas.
3. metode ini mampu mengurangi jumlah positif palsu yang terdeteksi dengan mempelajari perbedaan antara lalu lintas berbahaya dan tidak berbahaya,
4. dapat mengidentifikasi pola dan tren yang dapat mengindikasikan adanya serangan cyber dan Informasi yang diperoleh tersebut memiliki potensi untuk meningkatkan akurasi dalam intelijen ancaman.

1.4 Perumusan Masalah

Adapun beberapa point rumusan masalah yang di dapatkan dari penelitian ini, yaitu:

1. Seberapa efektif metode Convolutional Neural Network (CNN) dalam mendeteksi serangan cyber yang telah ada sejak lama dan yang baru muncul?
2. Bagaimana mengembangkan sistem deteksi serangan *cyber multi-classification* menggunakan metode *deep learning* CNN?

1.5 Batasan Masalah

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

1. Teknik yang digunakan untuk mendeteksi serangan cyber adalah algoritma CNN
2. Dataset yang digunakan dalam penelitian ini adalah CICDDoS2019, KDDCup1999, ISCX2012, dan NSL –KDD.

3. Pengembangan sistem akan dilakukan menggunakan bahasa pemrograman dan kerangka kerja yang sesuai untuk implementasi CNN dalam lingkungan deteksi serangan cyber.

1.6 Metodologi Penelitian

Berikut beberapa tahap metodelogi yang digunakan dalam melakukan penelitian ini yaitu:

1. Tahap Pertama (Studi Pustaka)

   Tahap pertama yang akan dilakukan dalam penelitian ini adalah mencari sumber pustaka-pustaka ilmiah yang berkaitan dengan topik laporan tugas akhir untuk menguatkan pembahasan yang sedang dilakukan.

2. Tahap Kedua (Perancangan Sistem)

   Tahap kedua adalah membahas tentang rancangan spesifikasi dalam penelitian ini. Dimana membuat suatu perancangan menggunakan pemodelan simulasi.

3. Tahap ketiga (Pengujian)

   Pada tahap ini, system yang telah dirancang akan dilakukan pengujian. Di dalam fase ini, menguji performa model menggunakan data uji. Validasi model bertujuan untuk memastikan bahwa model dapat mengenali berbagai jenis serangan cyber dengan akurasi yang tinggi.

4. Tahap keempat (Analisa)

   Lalu setelah hasil pengujian tersebut didapatkan maka akan dianalisa pada fase ini. Pada fase ini akan dilakukan analisis terhadap tingkat akurasi, kecepatan pemrosesan, dan kemampuan model dalam mengenali serangan cyber dengan tingkat keparahan yang berbeda.

5. Tahap kelima (Kesimpulan dan Saran)

   Di dalam Tahap ini, kesimpulan dari hasil uji dan analisa pembahasan akan dituangkan serta memberikan beberapa saran untuk acuan referensis jika riset ini ingin diteruskan.

1.7 Sistematika Penelitian

Untuk mempermudah dan memperjelas proses penyusunan pada tugas akhir dari setiap bab, maka dibuat sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pada bab satu ini terdiri dari penjelasan dengan cara sistematik mengenai topick riset yang diarnbil rneliputi latar belakng, tujuan dan manfaat, batasan dan perumusan masalah, metodelogi dan sistematiika penulisan.

BAB II TINJAUAN PUSTAKA

Di dalam bab dua ini beriskan tentang teori dasar dari riset yang berkaitan mengenai

BAB III METODOLOGI PENELITIAN

Kemudian pada bab tiga ini berisi penerangan secara bertahap tentang proses penelitian yang dillakukan. Penjabaran terssebut mengenai fase-fase perancangan system serta fase penerpan metodelogi riset.

BAB IV PENGUJIAN DAN ANALISIS

Lalu pada bab empat ini membahas tentang hasil pengujian dataset dimana dataset tersebut tlah dikerjakan saat pengerjaan tugas akhir. Hasilnya kemudian nanti dianalisa dari

BAB V KESIMPULAN

Kemudian pada bab terakhir ini berisikan konklusi akhir dari pembahasan research yang tlah dikerjakan. Serta ada pemberian saran yang dibutuhkan untuk pengembangan riset selanjutnya agar riset menjadi lebih menarik.

DAFTAR PUSTAKA

[1] M. C. Waxman, “International Law Commons, Internet Law Commons, Military, War, and Peace Commons, and the National Security Law Commons Recommended Citation Recommended Citation Matthew C. Waxman, Cyber Attacks as "Force," 2011. [Online]. Available: https://scholarship.law.columbia.edu/faculty_scholarshipAvailableat:https://scholarship.law.columbia.edu/faculty_scholarship/847

[2] J. N. Madubuike-Ekwe, “Cyberattack and the Use of Force in International Law,” *Beijing Law Review*, vol. 12, no. 02, pp. 631–649, 2021, doi: 10.4236/blr.2021.122034.

[3] Bojan Jovanovic, “Better Safe Than Sorry: Cyber Security Statistics and Trends for 2023.”

[4] Mike Mclean, “2023 Must-Know Cyber Attack Statistics and Trends.”

[5] “State of Cybercrime 2017: Security events decline, but not the impact | CSO Online.” Accessed: May 22, 2023. [Online]. Available: https://www.csoonline.com/article/3211491/state-of-cybercrime-2017-security-events-decline-but-not-the-impact.html

[6] Y. Zhou, M. Han, L. Liu, J. S. He, and Y. Wang, “Deep learning approach for cyberattack detection,” in *INFOCOM 2018 - IEEE Conference on Computer Communications Workshops*, Institute of Electrical and Electronics Engineers Inc., Jul. 2018, pp. 262–267. doi: 10.1109/INFCOMW.2018.8407032.

[7] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments,” *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/J.EGYR.2021.08.126.

[8] L. Cun *et al.*, “Handwritten Digit Recognition with a Back-Propagation Network.”

[9] M. Kravchik and A. Shabtai, “Detecting Cyberattacks in Industrial Control Systems Using Convolutional Neural Networks,” Jun. 2018, [Online]. Available: http://arxiv.org/abs/1806.08110

[10] Y. Lecun, Y. Bengio, and R. 4g332, “Convolutional Networks for Images, Speech, and Time-Series.”

[11] https://www.phishing.org/, “What Is Phishing?”

[12] “Denial of Service in sensor network”.

[13] T. A. Cahyanto, V. Wahanggara, D. Ramadana, and J. T. Informatika, “Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis.”

[14] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” 2005.

[15] M. Saxena, “CERIAS Tech Report 2007-04 SECURITY IN WIRELESS SENSOR NETWORKS-A LAYER BASED CLASSIFICATION Security in Wireless Sensor Networks A Layer-based Classification.”

[16] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” in *Ad Hoc Networks*, Elsevier, 2003, pp. 293–315. doi: 10.1016/S1570-8705(03)00008-8.

[17] Q. Wang, Y. Zhu, and L. Cheng, “Reprogramming wireless sensor network.”

[18] C. Ndubuisi, “Universitas Timur Laut (Shenyang, Cina)”, doi: 10.13140/RG.2.2.22752.81928.

[19] J. Clarke, “SQL Injection Attacks and Defense Second Edition.”

[20] A. Adeel, M. Gogate, and A. Hussain, “Contextual Audio-Visual Switching For Speech Enhancement in Real-World Environments,” Aug. 2018, doi: 10.1016/j.inffus.2019.08.008.

[21] T. Young, D. Hazarika, S. Poria, and E. Cambria, “Recent Trends in Deep Learning Based Natural Language Processing,” Aug. 2017, [Online]. Available: http://arxiv.org/abs/1708.02709

[22] H. Tian, S. C. Chen, and M. L. Shyu, “Evolutionary Programming Based Deep Learning Feature Selection and Network Construction for Visual Data Classification,” *Information Systems Frontiers*, vol. 22, no. 5. Springer, pp. 1053–1066, Oct. 01, 2020. doi: 10.1007/s10796-020-10023-6.

[23] M. M. Saeed, Z. Al Aghbari, and M. Alsharidah, “Big data clustering techniques based on Spark: a literature review,” *PeerJ Comput Sci*, vol. 6, pp. 1–28, 2020, doi: 10.7717/PEERJ-CS.321.

[24] K. Arulkumaran, M. P. Deisenroth, M. Brundage, and A. A. Bharath, “A Brief Survey of Deep Reinforcement Learning,” Aug. 2017, doi: 10.1109/MSP.2017.2743240.

[25] Z. W. 1 b, J. K. b, L. M. b, A. S. b, B. S. b, T. L. b, X. W. b, G. W. b, J. C. c, T. C. c Jiuxiang Gu a, “Recent advances in convolutional neural networks,” *sciencedirect*, vol. 77, pp. 354–377, May 2018.

[26] D. H. Hubel and A. T. N. Wiesel, “54 With 2 plate and 20 text-ftgutre8 Printed in Gret Britain RECEPTIVE FIELDS, BINOCULAR INTERACTION AND FUNCTIONAL ARCHITECTURE IN THE CAT’S VISUAL CORTEX,” 1962.

[27] L. Alzubaidi *et al.*, “Review of deep learning: concepts, CNN architectures, challenges, applications, future directions,” *J Big Data*, vol. 8, no. 1, Dec. 2021, doi: 10.1186/s40537-021-00444-8.

[28] R. M. S. E. Sagnik Basumallik, “Packet-data anomaly detection in PMU-based state estimator using convolutional neural network,” vol. Volume 107, pp. 690–702, May 2019.

[29] Mark A.Hall “Correlation-based Feature Selection for Machine Learning”

[30] C. Thomas, V. Sharma, and N. Balakrishnan, “Usefulness of DARPA Dataset for Intrusion Detection System Evaluation.”

[31] A. Dosovitskiy *et al.*, “An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale,” Oct. 2020, [Online]. Available: http://arxiv.org/abs/2010.11929

[32] “The CAIDA Anonymized Internet Traces Dataset (April 2008 - January 2019).”

[33] 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, May 2022, doi: 10.11591/ijeecs.v26.i2.pp1165-1172.

[34] J. Liang, W. Zhao, and W. Ye, “Anomaly-based web attack detection: A deep learning approach,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Dec. 2017, pp. 80–85. doi: 10.1145/3171592.3171594.

[35] https://www.unb.ca/cic/datasets/nsl.html, “NSL-KDD dataset.”

[36] B. Ingre and A. Yadav, “Performance analysis of NSL-KDD dataset using ANN,” in *International Conference on Signal Processing and Communication Engineering Systems - Proceedings of SPACES 2015, in Association with IEEE*, Institute of Electrical and Electronics Engineers Inc., Mar. 2015, pp. 92–96. doi: 10.1109/SPACES.2015.7058223.

[37] V. Kanimozhi and T. P. Jacob, “Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing,” *ICT Express*, vol. 7, no. 3, pp. 366–370, Sep. 2021, doi: 10.1016/j.icte.2020.12.004.