# KLASIFIKASI SERANGAN *PORT SCANNING* PADA *INTRUSION DETECTION SYSTEM* MENGGUNAKAN METODE LSTM (*LONG SHORT TERM MEMORY*)

**SKRIPSI**

**Diajukan untuk melengkapi salah satu syarat**
**memperoleh gelar sarjana Komputer**


**OLEH:**

**JUMHADI**
**09011281823038**

**JURUSAN SISTEM KOMPUTER**
**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS SRIWIJAYA**
**2022**

# HALAMAN PENGESAHAN

**KLASIFIKASI SERANGAN *PORT SCANNING* PADA *INTRUSION DETECTION SYSTEM* MENGGUNAKAN METODE LSTM (*LONG SHORT TERM MEMORY*)**

**SKRIPSI**

**Program Studi Sistem Komputer**

**Jenjang S1**

**Oleh :**

**JUMHADI**

**09011281823038**

**Indralaya, Agustus 2022**

**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

***CLASSIFICATION OF PORT SCANNING ATTACKS ON INTRUSION DETECTION SYSTEM USING METHOD LSTM (LONG SHORT TERM MEMORY)***

**FINAL TASK**

**Submitted to Complete One of the**

**ConditionsObtaining Strata 1 Degree**

**By**

**JUMHADI**

**09011281823038**

**Indralaya, Agustus 2022**

**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 : 22 Juni 2022

**Tim Penguji :**

1. **Ketua : Ahmad Zarkasi, M.T.**
2. **Sekretaris : Tri Wanda Septian, S.Kom., M.Sc.**
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 : Jumhadi

NIM 09011381823078

Judul : Klasifikasi serangan *Port Scanning* pada *Intrusion Detection System* menggunakan metode LSTM (*Long Short Term Memory*)

**Hasil Pengecekan Software iThenticate/Turnitin : 5%**

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

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaandari siapapun.

**Indralaya, Agustus 2022**


**Jumhadi**
**NIM.090111823038**

# KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Ungkapan syukur penulis panjatkan kepada Allah SWT, atas limpahan nikmat, rahmat, serta hidayah-nya sehingga penulis dapat menyelesaikan penyusunan tugas akhir ini yang berjudul **"Klasifikasi serangan *Port Scanning* pada *Intrusion Detection System* menggunakan metode LSTM (*Long Short Term Memory*)"**.

Dalam laporan ini penulis menjelaskan bagaimana proses klasifikasi dari serangan Port Scanning yang disertai data-data dan hasil yang diperoleh. Penulis berharap laporan ini bermanfaat bagi banyak pihak, serta menjadi salah satu sumber bacaan atau referensi bagi akademisi dan peneliti lain yang sedang menekuni bidang citra.

Penulis mendapatkan ide, saran dan bantuan dalam penyusunan laporan ini dari banyak pihak. Oleh karena itu, dalam kesempatan ini penulis ucapkan rasa syukur kepada Allah SWT dan rasa terima kasih penulis kepada semua pihak yang terhormat, antara lain:

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga saya dapat menyelesaikan penulisan tugas akhir ini dengan baik.

2. Kedua orang tua serta keluarga yang selalu mendoakan, nasihat, dukungan, moril dan material,

3. Yang terhormat, bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.

4. Yang terhormat, bapak Dr. Ir. H. Sukemi, M.T., selaku ketua jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

5. Yang terhormat, Bapak Ahmad Heryanto, S.Kom., M.T. selaku pembimbing tugas akhir yang selalu meluangkan waktu memberikan bimbingan, arahan dan dukungan dalam menyelesaikan tugas akhir.

6. Yang terhormat, bapak Rossi Passarella, M.ENG selaku Pembimbing Akademik Jurusan Sistem Komputer.

7. Mbak Reni selaku admin jurusan sistem komputer yang telah membantu mengurus seluruh berkas.

8. Kepada teman-teman tim penelitian COMNET khususnya yang telah mendukung penulis dalam menyelesaikan tugas akhir.

9. Kepada Kak Ahmad Afidin, S.Kom., Kak Lisa Melinda, S. Kom, selaku kakak tingkat yang memberikan referensi serta arahannya. Yusdiansya Putra, M. Taufik, Hanna Pertiwi, Tri Putri Rahmadani dan Caturning Anjarwati sebagai teman seperjuangan yang sangat baik, mulai dari diskusi, waktu dan saling mendukung satu sama lain sehingga penulis dapat menyelesaikan tugas akhir ini dengan baik.

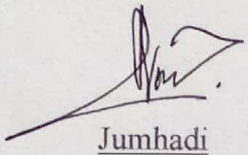
10. Terkhusus kepada Ika Damayanti yang selalu mendukung dan menyemangati penulis dalam menyelesaikan tugas akhir.

11. Semua pihak yang telah membantu.

Penulis menyadari bahwa penelitian ini masih jauh dari kata sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang bersifat membangun agar lebih baik lagi dikemudian hari. Akhir kata dengan segala keterbatasan, penulisa berharap semoga laporan ini menghasilkan sesuatu yang bermanfaat bagi kita semua.

Wassalamu'alaikumWarahmatullahi Wabarakatuh

Indralaya, Agustus 2022



Jumhadi

NIM.09011281823038

# HALAMAN PERSEMBAHAN

Skripsi saya yang berjudul "Klasifikasi serangan *Port Scanning* pada *Intrusion Detection System* menggunakan metode LSTM (*Long Short Term Memory*)", saya persembahkan untuk:

- Orang tua saya tercinta
- Pasangan saya tercinta
- Dosen Pembimbing
- Dosen Penguji
- Seluruh Dosen dan Staf jurusan Sistem Komputer
- Teman-teman satu angkatan Sistem Komputer 2018
- Teman-teman Sistem Komputer kelas B angkatan 2018
- Adik-adik tingkat jurusan Sistem Komputer

Semoga bermanfaat dan menjadi referensi bagi para pembaca sekalian.

# *CLASSIFICATION OF PORT SCANNING ATTACKS ON INTRUSION DETECTION SYSTEM USING METHOD LSTM (LONG SHORT TERM MEMORY)*

**JUMHADI (09011281823038)**
*Computer Engineering Department, Computer Science Faculty, SriwijayaUniversity*

Email: jumhadixcastle2015@gmail.com

## ABSTRACT

*Port Scanning is an attack that is carried out to identify open ports on a computer network system, open ports are also called listening ports, which are ports whose job is to receive incoming packets and also function to interact with outside networks. Port Scanning is included in the information gathering stage. Port Scanning attacks on computer networks today are still very difficult to detect because the attack pattern of Port Scanning does not establish a full connection to its target destination. This study classifies Port scanning attacks on the Intrusion Detection System using the Long Short Term Memory (LSTM) method, using the Port Scanning dataset on CSE-CIC-IDS2017. In this study, the Principal Component Analysis feature selection was applied to reduce the dimensions and also the efficiency of training time, Hyperparameter Tuning was also applied to see the best parameters to be applied to the research model, Research validation was carried out 5 times in the study. The best validation results from the overall results are 80% training data and 20 testing data where in this study the results obtained were 99.89% accuracy points, 99.88% recall, 99.90% specificity, 99.87% precision and F1 score 99, 88% and efficient training time is only 3 hours because of the use of PCA in the study.*

***Keywords*** : *Port Scanning, Principal Component Analysis, Tuning Hyperparameter*, LSTM (*Long Short Term Memory*).

***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** |

# KLASIFIKASI SERANGAN *PORT SCANNING* PADA *INTRUSION DETECTION SYSTEM* MENGGUNAKAN METODE LSTM (*LONG SHORT TERM MEMORY*)

**JUMHADI (09011281823038)**
Jurusan Sistem Komputer, Fakultas Ilmu Komputer,
Universitas SriwjayaEmail :
jumhadixcastle2015@gmail.com

## ABSTRAK

*Port Scanning* adalah sebuah serangan yang dilakukan untuk mengidentifikasi *port* yang terbuka pada sebuah sistem jaringan komputer, *port* terbuka disebut juga *listening port*, merupakan *port* yang bertugas untuk menerima paket masuk dan juga berfungsi untuk berinteraksi dengan jaringan luar. *Port Scanning* termasuk kedalam tahapan *information gathering*. Serangan *Port Scanning* pada jaringan komputer saat ini masih sangat sulit untuk dideteksi karena pola serangan dari *Port Scanning* tidak membangun koneksi penuh pada target tujuannya. Penelitian ini melakukan klasifikasi serangan *Port scanning* pada Intrusion Detection System menggunakan metode *Long Short Term Memory* (LSTM), menggunakan dataset *Port Scanning* pada CSE-CIC-IDS2017. Pada penelitian ini terapkan seleksi fitur *Principal Component Analysis* untuk mereduksi dimensi dan juga efisiensi waktu pelatihan, diterapkan juga Tuning Hyperparameter untuk melihat parameter terbaik untuk diterapkan pada model penelitian, Validasi penelitian dilakukan sebanyak 5 kali dalam penelitian. Hasil Validasi terbaik dari keseluruhan hasil yaitu pada 80% data training dan 20 data testing dimana pada penelitian ini didapatkan hasil poin akurasi 99,89%, recall 99,88%, spesifitas 99,90% presisi 99,87% dan F1 score 99,88% dan efisien waktu pelatihan menjadi 3 jam saja karena penggunaan PCA pada penelitian.

**Kata Kunci** : *Port Scanning*, *Principal Component Analysis*, *Tuning Hyperparameter*, LSTM (*Long Short Term Memory*).

**Mengetahui,**

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

# DAFTAR ISI

**Halaman**

# DAFTAR GAMBAR

**Halaman**

# DAFTAR TABEL

**Halaman**

# DAFTAR LAMPIRAN

# BAB I
# PENDAHULUAN

## 1.1. Latar Belakang

Perkembangan teknologi yang terjadi saat ini sangatlah pesat dengan adanya fasilitas internet yang mendukung dan perangkat yang memadai bagi setiap penggunanya, namun dibalik itu semua ada hal-hal negatif yang dapat menimbulkan dampak kerugian pada pihak pengguna internet itu sendiri, seperti contohnya serangan dari pihak-pihak yang tidak bertanggung jawab yang disebut dengan hacker. Ada banyak sekali tipe serangan yang dilakukan oleh para hacker untuk masuk ke suatu sistem jaringan komputer tujuannya, akan tetapi tipe serangan yang paling sering digunakan oleh para hacker sebelum masuk ke jaringan komputer tujuannya adalah dengan melakukan serangan *Port Scanning*. *Port Scanning* termasuk kedalam tahapan *information gathering*. Dalam tahap *information gathering* pada jaringan target, tentu banyak sekali informasi yang didapat, contohnya seperti identifikasi *port* pada jaringan tujuan, informasi tentang layanan yang berjalan, status pada jaringan komputer, sistem operasi yang digunakan, memori yang ditempati, dan memproses informasi targetnya, dari banyak informasi yang didapat tersebut, informasi utama yang paling di targetkan dari penerapan serangan *Port Scanning* ialah identifikasi port. *Port Scanning* adalah sebuah serangan yang dilakukan untuk menidentifikasi *port* yang terbuka pada sebuah sistem jaringan komputer, *port* terbuka disebut juga *listening port*, merupakan *port* yang bertugas untuk menerima paket masuk dan juga berfungsi untuk berinteraksi dengan jaringan luar [1].

Pada protocol jaringan TCP/IP, *port* merupakan mekanisme yang mendukung koneksi antar perangkat komputer lain, total 65.536 jenis *port* di dunia. Memilki 16 bit angka unik yang di sebut dengan *port number*. *Port* 445 (Microsoft-DS), *port* 80 (HTTP), dan *port* 443 (HTTPS) merupakan *port* yang paling sering ditarget hacker, tetapi semua jenis *port* terbuka berpotensi diserang oleh hacker. Port terbuka akan menjadi celah utama oleh para hacker untuk melakukan penyerangan lebih lanjut. Serangan *Port Scanning*

pada jaringan komputer saat ini masih sangat sulit untuk dideteksi karena pola serangan dari *Port Scanning* tidak membangun koneksi penuh pada target tujuannya, banyaknya paket dengan kombinasi non-standar dari flag TCP pada jaringan merupakan tanda dari serangan *Port Scanning*, meskipun ada beberapa cara untuk mencegah dan memblokir serangan *Port Scanning* namun tetap saja serangan *Port Scanning* menjadi ancaman serius yang sangat menakutkan, karena tidak ada serangan hacker yang tidak di awali *informasi gathering* dengan menggunakan *Port Scanning*, mengingat dari tahun ke tahun kasus kejahatan hacker terus meningkat hingga saat ini [2]. Berikut ini merupakan hasil penelitian terdahulu yang membahas mengenai serangan *Port Scanning* yang menjadi acuan utama untuk topik penelitian ini.

Pada penelitian [3] dengan judul penelitian Combating TCP Port Scan Attack penelitian menggunakan metode Sequential Neural Networks, penelitian ini menggunakan metode *Sequential Neural Networks* (SNN). Penelitian tersebut menggunakan dataset CAIDA. Pada penelitian ini mendapatkan performa yang baik yaitu dengan akurasi 97,51% dengan presisi 67% dan recall 70%. meskipun akurasi yang diperoleh pada penelitian ini cukup baik tetapi hasil yang diperoleh untuk presisi dan recall masih perlu ditingkatkan kembali.

Pada penelitian [4] dengan judul penelitian port-scan classification, penelitian ini menggunakan metode *Decision Tree Learning Algorithm*. Penelitian mendapatkan performa presisi 70% dan recall of 67%. penelitian ini menggunakan dataset Internet Scan Data Acquisition System (ISDAS). Namun performa yang diperoleh pada hasil presisi dan recall pada penelitian ini masih perlu ditingkatkan lagi mengingat hasilnya masih tergolong rendah.

Pada penelitian [5] dengan judul penelitian Efficient classification of portscan, Penelitian ini menggunakan algoritma *machine learning* dengan metode *Support Vector Machine* (SVM) dalam melakukan proses klasifikasi serangannya, penelitian ini memiliki performa yang baik dengan akurasi yang didapat 96.51%. Penelitian ini menggunakan dataset NSL-

KDD, namun penelitan tidak menggunakan seleksi fitur pada data penelitiannya sehingga hasil penilitian ini masih belum sempurna dan masih dapat di tingkat lagi hasilnya.

Pada penelitian [6] dengan judul penelitian portscan Attack Detection, penelitian ini menggunakan metode LSTM (*Long Short Term Memory*), memperoleh performa yang baik pada akurasi 98,90%. Penelitian ini menggunakan dataset CSE-CIC-IDS2017, pemilihan fungsi aktivasi penelitian [6] harus diperhatikan lagi karena perbandingan hasil tidak ditampilkan pada pembahasannya meskipun hasil yang di peroleh relu masih jauh di bawah fungsi aktivasi *tahn* dan sigmoid .

Dari beberapa penelitian terduhulu yang sudah di jelaskan pada pembahasan sebelumnya untuk hasil dan juga performa dari metode yang di gunakan, maka peneliti ini mengangkat judul klasifikasi serangan *Port Scanning* pada *intrusion detection system* menggunakan metode LSTM (*Long Short Term Momory*) mengunakan dataset CSE-CIC-IDS2017.

## 1.2. Rumusan Masalah

Berdasarkan penjelasan dari latar belakang yang sudah disampaikan diatas, maka penelitian ini akan melakukan klasifikasi serangan *Port Scanning* menggunakan metode *Long Short Term Momory* (LSTM), tidak seperti pada penelitian [5] yang tidak menerapkan seleksi fitur, penelitian ini menerapkan seleksi fitur Principal Component Analysis (PCA). Dalam penerapan penelitian ini juga akan di lakukan *Tuning Hypeparameter* untuk menentukan parameter terbaik untuk diterapkan pada penenlitian dan juga akan dilakukan uji validasi terhadap nilai akurasi, recall, spesifitas, precision, dan F1-Score.

## 1.3. Batasan Masalah

Adapun batasan masalah penelitian sebagai berikut :

1. Penelitian yang dilakukan berfokus untuk klasifikasi serangan *Port Scanning* dan non-serangan.
2. Menerapkan teknik dari metode LSTM (*Long Short Term Memory*).
3. Tidak dilakukan pencegahan terhadap serangan *Port Scanning.*
4. Menggunakan dataset CSE-CIC-IDS2017 yang di terbitkan oleh University of New Brunswick (UNB).

## 1.4. Tujuan

Adapun tujuan penelitian sebagai berikut:

1. Menerapkan seleksi fitur PCA untuk mereduksi dimensi untuk mengoptimalkan proses klasifikasi serangan *Port Scanning* dan non-serangan.
2. Menerapkan metode LSTM dalam klasifikasikan dari serangan *Port Scanning.*
3. Mengetahui performa klasifikasi berdasarkan akurasi, presisi, spesifitas ,recall dan F1-Score.

## 1.5. Manfaat

Berikut merupakan manfaat untuk penelitian ini:

1. Mengoptimalkan proses klasifikasi dengan PCA.
2. Menerapkan metode LSTM dalam penelitian selanjutnya.
3. Hasil performa klasifikasi dengan metode *Long Short Term Memory* (LSTM).

## 1.6. Metodologi Penelitian

Untuk metodologi penelitian melalui beberapa tahapan dalam penelitian ini melingkupi :

1. Metode Studi Pustaka dan Literature

Pada bagian ini peneliti mengumpulkan data mengenai cara maupun proses klasifikasi menggunakan dengan metode LSTM dari berbagai sarana ilmu membantu pembuatan Tugas Akhir ini.

2. Metode Konsultasi

Pada bagian ini, mengacu pada bagian-bagian yang sudah memiliki pengetahuan dan pemahaman yang baik untuk mengatasi masalah yang dihadapi saat peneliti menulis.

3. Metode Pengumpulan data

Pada langkah ini, dikumpulkan data mengenai serangan port scan, skema intruksi deteksi, dan proses pengklasifikasian.

4. Metode Pengujian

Pada Langkah ini pembuatan suatu rancang sistematis untuk training klasifikasi untuk dataset Port Scanning dan mendapatkan hasil.

5. Metode Analisis dan Kesimpulan

Berikutnya langkah terakhir pada penelitian ini, metode di analisis pada tahap klasifikasian dan penarikan beberapa kesimpulan untuk penelitian ini .

## 1.7. Sistematika Penulisan

Sistematika penulisan pada penelitian ini sebagai berikut:

**BAB I. PENDAHULUAN**

Dalam bab I, Membahas latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat pada penelitian, metode penelitian dan sistematika penulisan.

**BAB II. TINJAUAN PUSTAKA**

Dalam bab II, mencakup pembahasan tentang teori mendasar LSTM, Port scan, dan teori relevan lainnya untuk tugas akhir ini.

**BAB III. METODOLOGI**

Dalam bab III, meliputi tahap peneliti yang kerjakan dan pembangunan sistem klasifikasi dan menerapan metodologi penelitian tugas akhir.

**BAB IV. HASIL DAN ANALISIS**

Dalam bab IV, mencakup tahap peneliti untuk melihat performa dari sistem dan analisis dari metode LSTM .

**BAB V. KESIMPULAN DAN SARAN**

Dalam bab V, terdapat kesimpulan dan saran di tarik pada pembahasan sebelumnya dan membagikan beberapa masukan sebagai referensi.

# DAFTAR PUSTAKA


[1] M. Aamir, S. S. H. Rizvi, M. A. Hashmani, M. Zubair, and J. A. . Usman, "Machine Learning Classification of Port Scanning and DDoS Attacks: A Comparative Analysis," *Mehran Univ. Res. J. Eng. Technol.*, vol. 40, no. 1, pp. 215–229, 2021, doi: 10.22581/muet1982.2101.19.

[2] J. Gadge and A. A. Patil, "Port scan detection," *Proc. 2008 16th Int. Conf. Networks, ICON 2008*, 2008, doi: 10.1109/ICON.2008.4772622.

[3] B. Hartpence and A. Kwasinski, "Combating TCP Port Scan Attacks Using Sequential Neural Networks," *2020 Int. Conf. Comput. Netw. Commun. ICNC 2020*, pp. 256–260, 2020, doi: 10.1109/ICNC47757.2020.9049730.

[4] H. Kikuchi, N. Fukuno, T. Kobori, M. Terada, and T. Pikulkaew, "Automated port-scan classification with decision tree and distributed sensors," *J. Inf. Process.*, vol. 16, pp. 165–175, 2008, doi: 10.2197/ipsjjip.16.165.

[5] M. Vidhya, "Efficient classification of portscan attacks using Support Vector Machine," *2013 Int. Conf. Green High Perform. Comput. ICGHPC 2013*, 2013, doi: 10.1109/ICGHPC.2013.6533915.

[6] M. D. Hossain, H. Ochiai, D. Fall, and Y. Kadobayashi, "LSTM-based Network Attack Detection: Performance Comparison by Hyper-parameter Values Tuning," *Proc. - 2020 7th IEEE Int. Conf. Cyber Secur. Cloud Comput. 2020 6th IEEE Int. Conf. Edge Comput. Scalable Cloud, CSCloud-EdgeCom 2020*, pp. 62–69, 2020, doi: 10.1109/CSCloud-EdgeCom49738.2020.00020.

[7] X. Deng, Q. Liu, Y. Deng, and S. Mahadevan, "An improved method to construct basic probability assignment based on the confusion matrix for classification problem," *Inf. Sci. (Ny).*, vol. 340–341, pp. 250–261, 2016, doi: 10.1016/j.ins.2016.01.033.

[8] J. Dai, C. Chen, and Y. Li, "A backdoor attack against LSTM-based text classification systems," *IEEE Access*, vol. 7, pp. 138872–138878, 2019, doi: 10.1109/ACCESS.2019.2941376.

[9] D. Wu, Z. Jiang, X. Xie, X. Wei, W. Yu, and R. Li, "LSTM Learning with Bayesian and Gaussian Processing for Anomaly Detection in Industrial IoT," *IEEE Trans. Ind. Informatics*, vol. 16, no. 8, pp. 5244–5253, 2020, doi: 10.1109/TII.2019.2952917.

[10] P. S. Muhuri, P. Chatterjee, X. Yuan, K. Roy, and A. Esterline, "Using a long short-term memory recurrent neural network (LSTM-RNN) to classify network attacks," *Inf.*, vol. 11, no. 5, pp. 1–21, 2020, doi: 10.3390/INFO11050243.

[11] A. Muslim, A. B. Mutiara, R. Refianti, C. M. Karyati, and G. Setiawan,

"Comparison of accuracy between long short-term memory-deep learning and multinomial logistic regression-machine learning in sentiment analysis on twitter," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 2, pp. 747–754, 2020, doi: 10.14569/ijacsa.2020.0110294.

[12] C. Song, Y. Sun, G. Han, and J. J. P. C. Rodrigues, "Intrusion detection based on hybrid classifiers for smart grid," *Comput. Electr. Eng.*, vol. 93, no. September 2020, p. 107212, 2021, doi: 10.1016/j.compeleceng.2021.107212.

[13] N. Gupta, V. Jindal, and P. Bedi, "LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system," *Comput. Networks*, vol. 192, no. December 2020, p. 108076, 2021, doi: 10.1016/j.comnet.2021.108076.

[14] 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.

[15] S. Pletinckx and V. Ghi, "Classification of Distributed Strategies for Port Scan Reconnaissance."

[16] S. S. Panwar, P. S. Negi, and Y. P. Raiwani, "Implementation of machine learning algorithms on cicids-2017 dataset for intrusion detection using WEKA," *Int. J. Recent Technol. Eng.*, vol. 8, no. 3, pp. 2195–2207, 2019, doi: 10.35940/ijrte.C4587.098319.

[17] A. Fernández, S. García, F. Herrera, and N. V. Chawla, "SMOTE for Learning from Imbalanced Data: Progress and Challenges, Marking the 15-year Anniversary," *J. Artif. Intell. Res.*, vol. 61, pp. 863–905, 2018, doi: 10.1613/jair.1.11192.

[18] M. Qiao and H. Li, "Application of PCA-LSTM model in human behavior recognition," *J. Phys. Conf. Ser.*, vol. 1650, no. 3, 2020, doi: 10.1088/1742-6596/1650/3/032161.

[19] P. P. Lid and S. Planning, *PRINCIPAL COMPONENTS ANALYSIS ( PCA )* Xln 1*, vol. 19, no. 3. 1993.

[20] M. Aamir and S. M. Ali Zaidi, "Clustering based semi-supervised machine learning for DDoS attack classification," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 33, no. 4, pp. 436–446, 2021, doi: 10.1016/j.jksuci.2019.02.003.

[21] A. Rehman, A. Khan, M. A. Ali, M. U. Khan, S. U. Khan, and L. Ali, "Performance Analysis of PCA, Sparse PCA, Kernel PCA and Incremental PCA Algorithms for Heart Failure Prediction," *2nd Int. Conf. Electr. Commun. Comput. Eng. ICECCE 2020*, no. June, pp. 1–5, 2020, doi: 10.1109/ICECCE49384.2020.9179199.

[22] R. W. Kadhim and M. T. Gaata, "A hybrid of CNN and LSTM methods for securing web application against cross-site scripting attack," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 2, pp. 1022–1029, 2020, doi: 10.11591/ijeecs.v21.i2.pp1022-1029.

[23] Y. Zhang, “Artificial intelligence governance capability association model based on closed-loop control theory,” vol. 2020, pp. 1063–1067, 2020, doi: 10.1109/ITAIC49862.2020.9338966.

[24] C. J. Huang, M. C. Liu, S. S. Chu, and C. L. Cheng, “Application of machine learning techniques to Web-based intelligent learning diagnosis system,” *Proc. - HIS’04 4th Int. Conf. Hybrid Intell. Syst.*, pp. 242–247, 2005, doi: 10.1109/ichis.2004.25.

[25] H. I. Bülbül and Ö. Ünsal, “Comparison of classification techniques used in machine learning as applied on vocational guidance data,” *Proc. - 10th Int. Conf. Mach. Learn. Appl. ICMLA 2011*, vol. 2, pp. 298–301, 2011, doi: 10.1109/ICMLA.2011.49.

[26] P. Ongsulee, “Artificial intelligence, machine learning and deep learning,” *Int. Conf. ICT Knowl. Eng.*, pp. 1–6, 2018, doi: 10.1109/ICTKE.2017.8259629.

[27] M. U. Kim and H. Jong Yang, “RNN-Based Node Selection for Sensor Networks with Energy Harvesting,” *9th Int. Conf. Inf. Commun. Technol. Converg. ICT Converg. Powered by Smart Intell. ICTC 2018*, pp. 1316–1318, 2018, doi: 10.1109/ICTC.2018.8539707.

[28] Y. Lu, Y. Shi, G. Jia, and J. Yang, “A new method for semantic consistency verification of aviation radiotelephony communication based on LSTM-RNN,” *Int. Conf. Digit. Signal Process. DSP*, vol. 0, pp. 422–426, 2016, doi: 10.1109/ICDSP.2016.7868592.

[29] R. Anhar, T. B. Adji, and N. Akhmad Setiawan, “Question classification on question-answer system using bidirectional-LSTM,” *Proc. - 2019 5th Int. Conf. Sci. Technol. ICST 2019*, pp. 1–5, 2019, doi: 10.1109/ICST47872.2019.9166190.

[30] H. Zheng, F. Lin, X. Feng, and Y. Chen, “A Hybrid Deep Learning Model With Attention-Based Conv-LSTM Networks for Short-Term Traffic Flow Prediction,” *IEEE Trans. Intell. Transp. Syst.*, pp. 1–11, 2020, doi: 10.1109/tits.2020.2997352.

[31] P. J. Jino, J. John, and K. Balakrishnan, “Offline handwritten Malayalam character recognition using stacked LSTM,” *2017 Int. Conf. Intell. Comput. Instrum. Control Technol. ICICICT 2017*, vol. 2018-Janua, pp. 1587–1590, 2018, doi: 10.1109/ICICICT1.2017.8342807.