FRI-2G.302-1-CCT2-01

ANALYTICAL INSTRUMENTS FOR NETWORK TRAFFIC DIAGNOSTICS IN COMMUNICATIONS [11]

Assoc. Prof. Ivelina Balabanova, PhD
Department of Communications Equipment and Technologies
Technical University of Gabrovo, Bulgaria
Tel.: +359 896 640 473
E-mail: ivstoeva@abv.bg

Assoc. Prof. Georgi Georgiev, PhD
Department of Communications Equipment and Technologies
Technical University of Gabrovo, Bulgaria
Tel.: +359 887 522 029
E-mail: givanow@abv.bg

Abstract: *In recent years, the digital evolution of Artificial Intelligence (AI) and Machine Learning (ML) has created a fundamental analytical framework to support technological innovation activities in various industry sectors. The paper presents a review on the integration of AI and ML concepts in monitoring and diagnostic systems in ICT-based infrastructures. A classification of the models, methods, algorithms and phases of different types of Machine Learning tools is made. Approaches for extracting of informative features when processing objects and processes using Artificial Intelligence technology are synthesized. A categorization of intelligent tools for analyzing the state of network traffic and performance indices of the transmission medium in communications was compiled. The review covers three analytical aspects in raw data manipulation procedures, respectively clustering, classification and predictive analysis.*

Keywords: *Transmission Medium, Network Traffic Monitoring, Artificial Intelligence, Machine Learning, Deep Learning.*

ВЪВЕДЕНИЕ

Концепцията за технологично развитие на съвременния свят, подобно на аритметична прогресия, е силно базирана на Artificial Intelligence (AI). AI навлиза все повече във всички технически сфери на човешкото ежедневие, бизнеса, икономиката, информационните технологии и основни сфери на промишлеността. Machine Learning (ML) се дефинира като AI подобласт, където са комбинирани информационни клъстери и специализирани алгоритми за провеждане на обучение във връзка с прогнозиране или изработване на набори за многовариантен избор на решение. При ML няма необходимост от конкретни “explicitly programming” процедури (Blanck, S., 2021), (Tiwari, T., 2018). Аналитичните Deep Learning инструменти или Deep Neural Networks (DNNs) се разглеждат като част от ML методите, при които понятието “deep” се обвързва с „дълбочината на слоевете на невронните мрежи или съвкупността от изчислителни единици в структурните Multiple Hidden Layers“ (Alafi, B., 2019), (Korchi, A., Massaoudi, F., & Oughdir, L., 2019). Известни са четири базисни типа на обучение – “Supervised Learning”, “Unsupervised Learning”, “Semi-Supervised Learning” и “Reinforcement Learning”, на всеки, от които се причислява комплекс от аналитични методи и алгоритми (Фиг. 1) (Faouzi, J., & Colliot, O., 2022), (Sarker, I., 2021), (Yang, X., Song, Z., King, I., & Xu, Z., 2022), (Sahu, S., Mokhade, A., & Bokde, G., 2023).

[11] The paper was presented on 24 October 2025 in section “Communication and Computer Technologies” with original title in Bulgarian: АНАЛИТИЧНИ ИНСТРУМЕНТИ ЗА ДИАГНОСТИКА НА МРЕЖОВИЯ ТРАФИК В КОМУНИКАЦИИТЕ

Фиг. 1. Класификация на Machine Learning методи и алгоритми

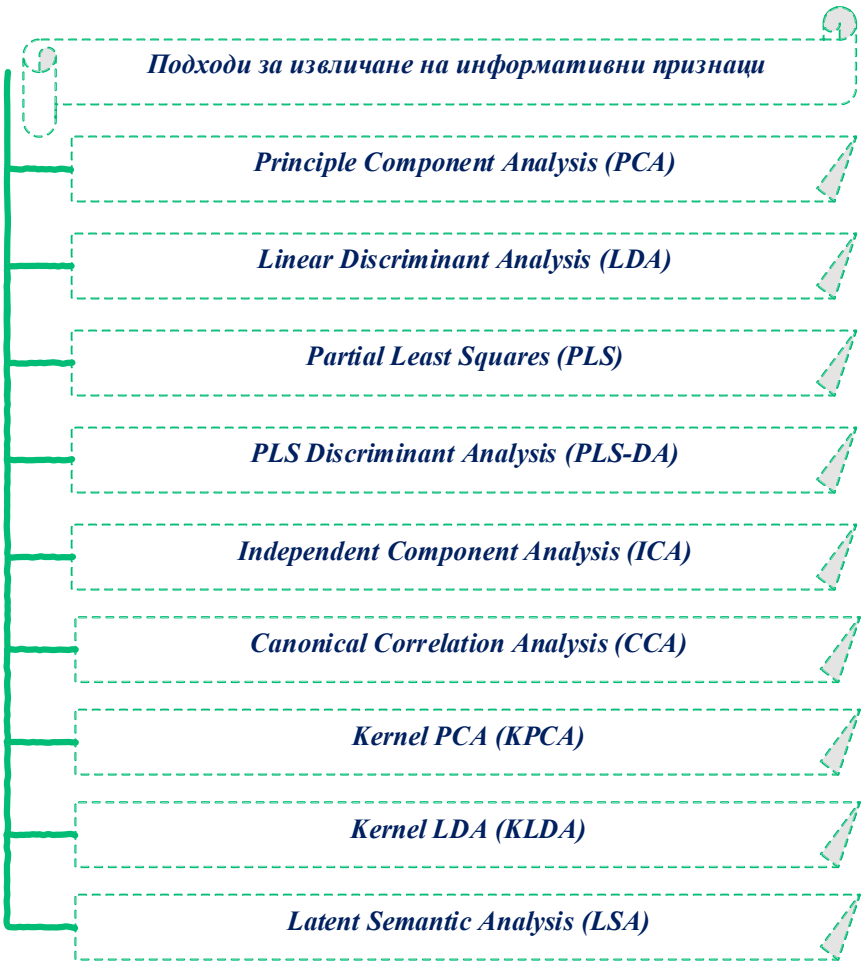
В доклада е проведена ретроспекция на основните компоненти, фази и инструменти в основата на Artificial Intelligence, Machine Learning и Deep Learning, приложими в съвременните комуникации при параметризация на преносната среда и процедури по мониторинг на мрежовия трафик.

ИЗЛОЖЕНИЕ

Инструменти за извличане на комплекс от специфични характеристики при обработка на масиви от данни

Подборът и прилагането на подходящи подходи за извличане на характеристики или “Feature Extraction Techniques” при обработка на целеви обекти като една от жизнените фази в AI и ML задачите за класификация, клъстеризация и прогнозен анализ са съществени за постигането на добра техническа рамка с висока ефективност. Направена е систематизация

на някои от най-често използваните инструменти в това направление, показана на Фиг. 2 (Suhaidi, M., Kadir, R., & Tiun, S., 2021), (Nurunnabi, A., Teferle, F., Laefer, D., Lindenbergh, R., & Hunegnaw, A., 2022), (Sweietlicka, I., Kuniszyk-Jozkowiak, W., & Swietlicki, M., 2022).

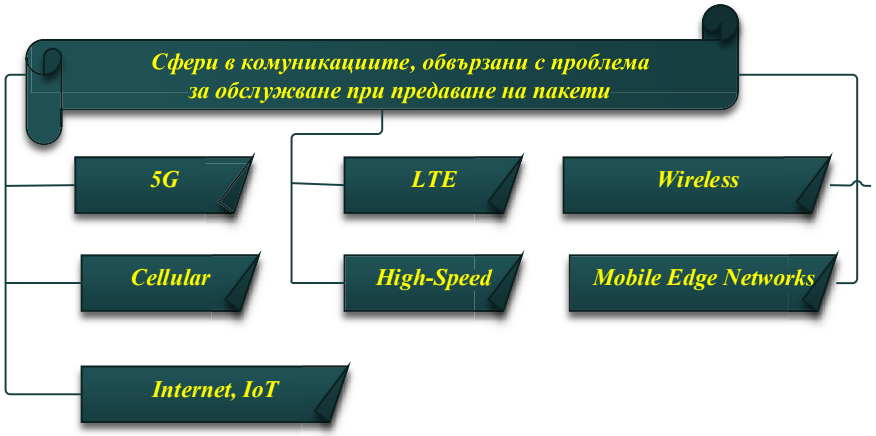


Фиг. 2. Feature extraction подходи при обработка на тестови AI и ML обекти

Инструменти за интелигентен анализ на състоянието и параметризацията на преносната среда в комуникационните системи

Ефективността на обслужване на пакетни данни в информационно-комуникационните системи е комплексен процес, основаващ се на редица фактори и параметри на преносната среда и използваните комуникационни канали за връзка. Проблемът е особено актуален по отношение на различни сфери в комуникациите, дадени на Фиг. 3 (Waller, J., 2014), (Ferreira, G., Ravazzi, C., Dabbene, F., Calafiore, G., & Fiore, M., 2023). Комплексният мониторинг на мрежовия трафик е една от основните дейности, регламентирани в политиките за достъп до информационни клъстери посредством WEB пространството на частни и корпоративни клиенти. По дефиниция се определя като многостранен процес за ефективно управление на трафичния поток, извършван от страна на:

- операторите „доставчици на Интернет услуга“;
- мрежовите администратори в учреждения;
- компании „клиенти“;
- различните регулаторни органи в сферата на информационното обслужване (Kaur, P., 2019), (Zhou, Y., Zhang, D., Gao, K., Sun, Ch., Cao, J., Wang, Y., Xu, M., & Wu, J., 2021).



Фиг. 3. Основни сфери в комуникациите, обвързани с проблема за обслужване при предаване на пакети

Основните направления в научните изследвания по отношение на анализ на мрежовия трафик обхваща различни процедури, които могат да се групират по начините на Фиг. 4 (Siracusano, G., Galea, S., Sanvito, D., Malekzadeh, M., Antichi, G., Costa, P., Haddadi, H., & Bifulco, R., 2022), (Lohrasbinasab, I., Shahraki, A., Taherkordi, A., & Jurcut, A., 2021), (Zhan, S., Yu, L., Wang, Z., Du, Y., Yu, Y., Cao, Q., Dang, S., & Khan, Z., 2021), (Awaforiaju, T., Lasisi, H., Olawuyi, A., & Olatunde, O., 2023), (Dodan, M., Vien, Q., & Nguyen, T., 2022), (Ferreira, G., Ravazzi, C., Dabbene, F., Calafiore, G., & Fiore, M., 2023). Особено съществен аспект е анализът и параметричната оценка на Интернет трафика, свързани с осигуряване на качеството на услугата при частни и корпоративни потребители по отношение на различни функции, онагледени на Фиг. 5 (Shahraki, A., Abbasi, M., Taherkordi, A., & Jercut, A., 2021). В качеството на основни комплексни направления се очертават:

- „повишаването на производителността“;
- „ефективните технологии за достъп, методи за защита“;
- „обезпечаване на обслужването на големи трафични потоци и буферното натрупване на информационни масиви“ (Vashishth, T., Sharma, V., Kumar, B., & Chaudhary, S., 2023), (Guo, A., & Yuan, Ch., 2021).

Широко използвани за различни сценарии при мониторинг и диагностика са комбинирани подходи с включване на конволюционни и рекурентни невронни мрежи (Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., & Lloret, J., 2017), (Salman, O., Elhajj, I., Kayssi, A., & Chehab, A., 2020). Други инструменти, използващи извлечени статистически трафични характеристики, са:

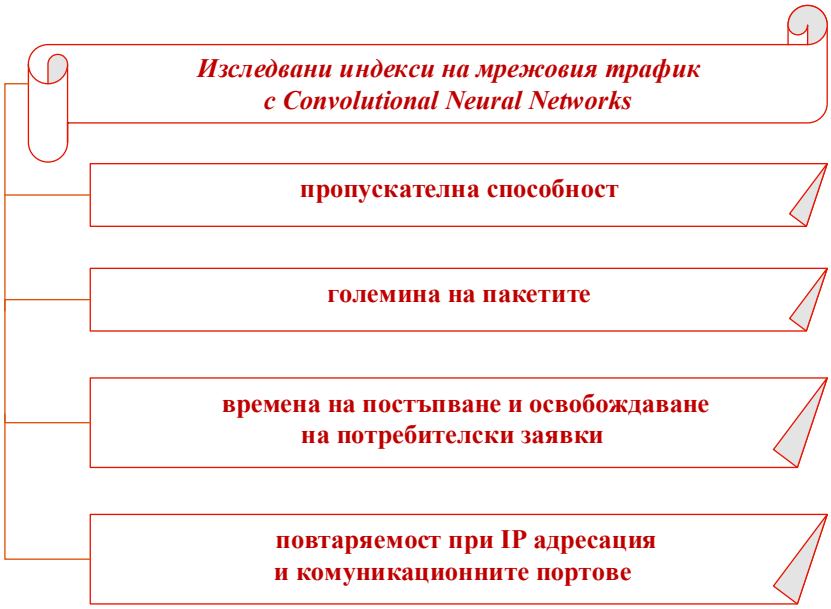
- Naïve Bayes алгоритъм;
- метод на опорните вектори (Support Vector Machine);
- линейни и квадратични дискриминантни класификатори (Revendran, R., & Menon, R., 2015), (Khater, N., & Overill, R., 2015).

В огромната си част съществуващите проучвания засягат детектиране и установяване на типа аномалии и нарушения в целостта на предаваната информация (Toupas, P., Chamou, D., Giannoutakis, K., Drosou, A., & Tzovaras, D., 2019), (Al-Turaiki, I., Altwaijry, N., Agil, A., Aljodhi, H., Alharbi, S., & Alqassem, L., 2020), (Aouedi, O., Piamrat, K., & Parrein, B., 2022). Рекурентните невронни мрежи RNN и една от основните им разновидности LSTM мрежите се прилагат при оценка на трафичните характеристики при подмрежовите енкодери. Често използван невронен апарат се явяват също конволюционните невронни мрежи CNN в ролята на способи за предотвратяване на кибератаки (Siracusano, G., Galea, S., Sanvito, D., Malekzadeh, M., Antichi, G., Costa, P., Haddadi, H., & Bifulco, R., 2022), (Ciptaningtyas, H., Fatichah, Ch., & Sabila, A., 2016).

Фиг. 4. Категории интелигентни инструменти за анализ на състоянието на мрежовия трафик

Фиг. 5. Аспекти при осигуряване на качество на услугата при частни и корпоративни клиенти

Могат да се посочат и процесите, свързани с диагностика на трафика и детектиране на аномалии от въздействия на зловреден софтуер с помощта на мрежи на базата Gradient Descent и Momentum алгоритми (Saber, M., Farissi, I., Chadli, S., & Emharraf, M., 2017). Проблемът с установяване на нарушения в мрежовия трафик е обект на цялостни системи в правителствени, административни и индустриални центрове по отношение на предлаганите от тях обществени услуги (Ilyas, M., & Alhabri, S., 2022). Друг аспект се свързва с подобряване на скалируемостта в интегрираните системни решения с машинно обучение при онлайн диагностика на мрежовия трафик (Antunes, M., Oliveira, L., Seguno, A., Verissimo, J., Salgado, R., & Murteira, T., 2022). Често CNN структурите са успешно използвани във връзка с измервани специфични параметри на мрежовия трафик, показани на Фиг. 6 (Freine, G., 2019), (Mihaylov, G., Iliev, T., Stoyanov, I., & Ivanova, E., 2022).



Фиг. 6. Изследвани индекси на мрежовия трафик с приложение на Convolutional Neural Networks

RNN невронните модели могат да бъдат полезни във връзка с класификация на криптиран трафик чрез:

- FTP (File Transfer Protocol);
- HTTP (Hyper-Text Transfer Protocol);
- VoIP (Voice Over Internet Protocol);
- XMPP (Extensible Messaging and Presence Protocol);

и други комуникационни протоколи и стандарти при безжичните сензорни мрежи (Aitken, W., & Brown, D., 2022). Съчетаването на CNNs и Long Short-Term Memory (LSTM) при опериране с VPN платформи дава възможност за ефективна идентификация на криптирано трафично съдържание, включващо гласови данни, изображения и други формати (Hu, X., Gu, Ch., & Wei, F., 2021). Описаният в (Umair, M., Iqbal, Z., Bilal, M., Nebhen, J., Almohamed, T., & Mehmood, R., 2022) подход, комбиниращ Deep Neural Networks (DNN) с k-Nearest Neighbors (k-NN) и Support Vector Machine (SVM), решава различни задачи, свързани с мониторинг на сигурността и откриване на проникванията по отношение на мрежи и мрежови сегменти от IoT устройства. Невронните структури на основата на „дълбоко обучение“, включващи:

- Multi-Layer Perceptrons,
- CNNs,
- RNNs,
- Generative Adversarial Networks (GAN),

са широко използвани при класификация на криптирано съдържание по отношение на известни Google Applications (Rezaei, Sh., & Iu, X., 2019). Bayesian Neural Networks се явяват невронен апарат, удовлетворяващ изискванията на мрежовите оператори във връзка с идентификацията на аномалии при предаване на трафични пакети (Michael, P., Valla, E., & Neggatu, N., 2017).

ЗАКЛЮЧЕНИЕ

Ефективността на прилаганите аналитични способи при различни процедури по диагностика на преносната среда е от съществено значение за подпомагане на дейностите на мрежовите разработчици в етап „планиране“ и администраторите във фазите „мониторинг, поддръжка и експлоатация“. Обследването на сегментите на комуникационните инфраструктури често изиска подходи на основата на съвкупност от инструменти за клъстерен анализ, идентификация и класификация на процеси и обекти, както и прогнозиране на измерими индекси на производителност като:

- „текущо време на постъпване“;
- „натоварване на работните станции“;
- „пропускателна способност“ и т.н.

Достоверността на резултати при Analytics, Artificial Intelligence, Machine Learning и Deep Learning апарати се потвърждава чрез верификация на комплекс от постигнати близки или сходни количествени критерии за оценка при:

- Клъстерен анализ: Silhouette score, Calinski-Harabasz index;
- Класификация: Accuracy, Precision, Recall, F1-score;
- Регресия: Mean Squared Error, Root Mean Squared Error, R-Squared.

REFERENCES

Aitken, W., & Brown, D. (2022). *Application Traffic Classification Using Neural Networks*. Canada: Defence Research and Development Canada.

Alafi, B. (2019). *Artificial Intelligence and Deep Learning Methodologies.* The Journal of Cognitive Systems, 4(2), pp. 57-61.

Al-Turaiki, I., Altwaijry, N., Agil, A., Aljodhi, H., Alharbi, S., & Alqassem, L. (2020). *Anomaly-Based Network Intrusion Detection Using Bidirectional Long Short-Term Memory and Convolutional Neural Network.* ISeSure, 12(3), pp. 37-44.

Antunes, M., Oliveira, L., Seguno, A., Verissimo, J., Salgado, R., & Murteira, T. (2022). *Benchmarking Deep Learning Methods for Behaviour-Based Network Intrusion Detection.* Informatics, 9(29), pp. 1-18.

Aouedi, O., Piamrat, K., & Parrein, B. (2022). *Intelligent Traffic Management in Next-Generation Networks.* HAL Open Science Feature Internet, 14(44), pp. 1-35.

Awaforiaju, T., Lasisi, H., Olawuyi, A., & Olatunde, O. (2023). *Artificial Neural Networks of Key Performance Indicators for Mobile Telecommunications.* Journal of Science and Technologies, 15(2), pp. 43-53.

Blanck, S. (2021). *Artificial Intelligence / Machine Learning Explained*. Stanford: Gordian Knot for National Security Innovation.

Ciptaningtyas, H., Fatichah, Ch., & Sabila, A. (2016). *Network Traffic Anomaly Prediction Using Artificial Neural Network*. Engineering International Conference, 5-6 October 2016, Semarang.

Dodan, M., Vien, Q., & Nguyen, T. (2022). *Internet Traffic Prediction Using Recurrent Neural Networks.* International Journal Endorsed Transactions on Industrial Networks and Intelligent Systems, 9(4), pp. 1-14.

Faouzi, J., & Colliot, O. (2022). *Classic Machine Learning Algorithms*. Paris: HAL Open Access.

Ferreira, G., Ravazzi, C., Dabbene, F., Calafiore, G., & Fiore, M. (2023). *Forecasting Network Traffic: A Survey and Tutorial with Open-Source Comparative Evaluation.* International Journal IEEE Access, 99(1), pp. 1-28.

Freine, G. (2019). *Deep Learning for the Analysis of Network Traffic Measurements*. Montevideo: Universidad de la Republica.

Guo, A., & Yuan, Ch. (2021). *Network Intelligent Control and Traffic Optimization Based on SDN and Artificial Intelligence.* Electronics, 10(6), pp. 1-20.

Hu, X., Gu, Ch., & Wei, F. (2021). *A Network Combining CNN and LSTM for Internet Encrypted Traffic Classification.* Hindawi, Security and Communication Networks, 2021, pp. 1-15.

Ilyas, M., & Alhabri, S. (2022). *Machine Learning Approaches to Network Intrusion Detection for Contemporary Internet Traffic.* Computing, 104(1), pp. 1-16.

Kaur, P. (2019). *A Methodical Review on Network Traffic Monitoring and Analysis Tools.* Journal of Composition Theory, 12(9), pp. 1964-1968.

Khater, N., & Overill, R. (2015). *Network Traffic Classification Techniques and Challenges*. 10th International Conference on Digital Information Management, 21-23 October 2015, Jeju.

Korchi, A., Massaoudi, F., & Oughdir, L. (2019). *Machine Learning and Deep Learning Revolutionize Artificial Intelligence.* International Journal of Scientific & Engineering Research, 10(9), pp. 1536-1539.

Lohrasbinasab, I., Shahraki, A., Taherkordi, A., & Jurcut, A. (2021). *From Statistical to Machine Leaning-Based Network Traffic Prediction.* International Journal Transactions on Emerging Telecommunications Technologies, 33(4), pp. 1-29.

Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., & Lloret, J. (2017). *Network Traffic Classifier with Convolutional and Recurrent Neural Networks for Internet of Things.* IEEE Access, 5, pp. 18042-18050.

Michael, P., Valla, E., & Neggatu, N. (2017). *Network Traffic Classification via Neural Networks*. Cambridge: University of Cambridge.

Mihaylov, G., Iliev, T., Stoyanov, I., & Ivanova, E. (2022). *An Approach for Point-to-Point Link within Mobile Network Coverage*. International Scientific Conference on Communications, Information, Electronic and Energy Systems, 25-27 November 2022, Ruse.

Nurunnabi, A., Teferle, F., Laefer, D., Lindenbergh, R., & Hunegnaw, A. (2022). *A Two-Step Feature Extraction Algorithm: Application to Deep Learning for Point Cloud Classification.* International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLVI-2/W1-2022, pp. 401-408.

Revendran, R., & Menon, R. (2015). *An Efficient Method for Internet Traffic Classification and Identification Using Statistical Features.* International Journal of Engineering Research & Technology, 4(7), pp. 297-303.

Rezaei, Sh., & Iu, X. (2019). *Deep Learning for Encrypted Traffic Classification: An Overview.* IEEE Communications Magazine, 57, pp. 76-81.

Saber, M., Farissi, I., Chadli, S., & Emharraf, M. (2017). *Performance Analysis of an Intrusion Detection Systems Based on Artificial Neural Network.* Advances in Intelligent Systems and Computing, 5(52), pp. 511-521.

Sahu, S., Mokhade, A., & Bokde, G. (2023). *An Overview of Machine Learning, Deep Learning, and Reinforcement Learning-Based Techniques in Quantitative Finance: Recent Progress and Challenges.* Applied Sciences, 13, pp. 1-27.

Salman, O., Elhajj, I., Kayssi, A., & Chehab, A. (2020). *Data Representation for CNN Based Internet Traffic Classification: A Comparative Study.* Multimedia Tools and Applications, 80, pp. 16951-16977.

Sarker, I. (2021). *Machine Learning: Algorithms, Real-World Applications and Research Directions.* SN COMPUT. SCI., 2(160), pp. 1-10.

Shahraki, A., Abbasi, M., Taherkordi, A., & Jercut, A. (2021). *Active Learning for Network Traffic Classification: A Technical Study.* IEEE Transactions on Cognitive Communications and Networking, 8(1), pp. 422-439.

Siracusano, G., Galea, S., Sanvito, D., Malekzadeh, M., Antichi, G., Costa, P., Haddadi, H., & Bifulco, R. (2022). *Re-Architecting Traffic Analysis with Neural Network Interface Cards*. 19th USENIX Symposium on Networked Systems Design and Implementation, 4-6 April 2022, Washington.

Suhaidi, M., Kadir, R., & Tiun, S. (2021). *A Review of Feature Extraction Methods on Machine Learning.* Journal of Information System and Technology Management, 6(22), pp. 51-59.

Sweietlicka, I., Kuniszyk-Jozkowiak, W., & Swietlicki, M. (2022). *Artificial Neural Networks Combined with the Principal Component Analysis for Non-Fluent Speech Recognition.* MDPI Sensors, 22(1), pp. 1-16.

Tiwari, T. (2018). *How Artificial Intelligence, Machine Learning and Deep Learning are Radically Different.* International Journals of Advanced Research in Computer Science and Software Engineering, 8(2), pp. 1-9.

Toupas, P., Chamou, D., Giannoutakis, K., Drosou, A., & Tzovaras, D. (2019). *An Intrusion Detection System for Multi-Class Classification Based on Deep Neural Networks*. 18th IEEE International Conference on Machine Learning and Applications, 16th-19th December 2019, Florida.

Umair, M., Iqbal, Z., Bilal, M., Nebhen, J., Almohamed, T., & Mehmood, R. (2022). *An Efficient Internet Traffic Classification System Using Deep Learning for IoT.* Computers, Materials & Continua, 71, pp. 407-422.

Vashishth, T., Sharma, V., Kumar, B., & Chaudhary, S. (2023). *Artificial Intelligence-Enabled Traffic Optimization: A Comprehensive Survey.* Journal of Industrial Engineering, 52(5), pp. 26-34.

Waller, J. (2014). *Performance Benchmarking of Application Monitoring Frameworks*. Kiel: Computer Science Series.

Yang, X., Song, Z., King, I., & Xu, Z. (2022). *A Survey on Deep Semi-Supervised Learning.* IEEE Transactions on Knowledge and Data Engineering, 35(9), pp. 8934-8954.

Zhan, S., Yu, L., Wang, Z., Du, Y., Yu, Y., Cao, Q., Dang, S., & Khan, Z. (2021). *Cell Traffic Prediction Based on Convolutional Neural Network for Software-Defined Ultra-Dense Visible Light Communication Networks.* International Journal of Security and Communication Networks, 1, pp. 1-10.

Zhou, Y., Zhang, D., Gao, K., Sun, Ch., Cao, J., Wang, Y., Xu, M., & Wu, J. (2021). *Intent-Driven Network Traffic Monitoring.* IEEE/ACM Transactions on Networking, 30(2), pp. 939-952.