DOI: 10.53469/jtpes.2024.04(03).18

Advanced Network Intrusion Detection with TabTransformer

Xiaosong Wang[1], Yuxin Qiao[2], Jize Xiong[3], Zhiming Zhao[4], Ning Zhang[5], Mingyang Feng[6], Chufeng Jiang[7]

[1]Computer Network Technology, Xuzhou University of Technology, Xuzhou, China
[2]Computer Information Technology, Northern Arizona University, Flagstaff, USA
[3]Computer Information Technology, Northern Arizona University, Flagstaff, USA
[4]Computer Science, East China University of Science and Technology, Shanghai, China
[5]Computer Science, University of Birmingham, Dubai, United Arab Emirates
[6]Computer Information Technology, Northern Arizona University, Flagstaff, USA
[7]Computer Science, The University of Texas at Austin, Fremont, USA
[1]wang138125@gmail.com; [2]yq83@nau.edu; [3]jasonxiong824@gmail.com; [4]zhiming817@gmail.com; [5]nxz243@alumni.bham.ac.uk; [6]zgjsntfmy@gmail.com; [7]chufeng.jiang@utexas.edu

Abstract: ***In today's digital era, the security of networked systems is of utmost importance amidst the increasing prevalence of cyber threats and sophisticated intrusion techniques. This paper addresses the critical need for robust network intrusion detection systems (NIDS) in today's digital landscape, amidst escalating cyber threats. Leveraging a dataset derived from a simulated military network environment, we explore various intrusion scenarios encountered in cyber warfare. Reviewing existing literature reveals a spectrum of methodologies, including anomaly-based and deep learning approaches. To enhance current methodologies, we propose a binary classification framework using TabTransformer, a transformer-based architecture, for network intrusion detection. We present detailed methodology, encompassing data preprocessing, model architecture, and evaluation metrics, with empirical results demonstrating the efficacy of our approach in mitigating cyber threats and enhancing network security.***

Keywords: Network security; Intrusion detection; TabTransformer.

1. INTRODUCTION

In today's interconnected digital landscape, ensuring the security and integrity of networked systems is paramount [1-2]. With the proliferation of cyber threats[3][4] and sophisticated intrusion techniques, the need for robust network intrusion detection systems (NIDS) has never been more critical. This paper addresses the challenge of network intrusion detection, focusing on the development and evaluation of effective methodologies to safeguard network infrastructures against malicious activities. The foundation of this research is built upon the analysis of a comprehensive dataset sourced from a simulated military network environment. This dataset emulates the complexities of a typical US Air Force LAN, providing a rich source of raw TCP/IP dump data reflecting real-world network behaviors. In this simulated environment, various intrusion scenarios were enacted, encompassing a spectrum of attack types commonly encountered in cyber warfare scenarios.

A comprehensive review of existing literature in network intrusion detection reveals a diverse landscape of methodologies and approaches. One set of studies delves into anomaly-based techniques, shedding light on the challenges and systems prevalent in network intrusion detection [1-2]. Another set of research proposes deep learning approaches tailored for intrusion detection, showcasing their efficacy in mitigating cyber threats [3-5]. Additionally, some studies leverage convolutional neural networks (CNNs) to bolster intrusion detection capabilities [6-8], highlighting the applicability of advanced neural architectures [9-10]. Comprehensive reviews offer insights into existing methodologies [11-15]. Other studies explore deep learning approaches for intrusion detection [16-22], emphasizing their potential for enhancing network security [23]. Several contributions to the discourse include surveys, systematic studies, and comparative analyses, providing valuable perspectives on the strengths and limitations of various intrusion detection techniques [24-28]. These limitations underscore the need for innovative approaches that can address the shortcomings of existing methodologies and provide scalable, efficient, and robust solutions for network intrusion detection.

In this study, we frame the problem of network intrusion detection as a binary classification task, wherein network connections are classified as either "Normal" or "Anomalous." Leveraging the wealth of features encapsulated within the dataset, our objective is to develop a robust and scalable intrusion detection model capable of accurately distinguishing between benign and malicious network traffic. To address the aforementioned challenges and capitalize on the rich feature space provided by the dataset, we propose the utilization of TabTransformer [29], a state-of-the-art transformer-based architecture. TabTransformer leverages the self-attention mechanism to effectively capture intricate patterns and dependencies within tabular data, making it particularly well-suited for the task of network intrusion detection. In the subsequent sections of this paper, we provide a detailed exposition of our methodology, encompassing data preprocessing, model architecture, training procedure, and evaluation metrics. Furthermore, we present empirical results and comparative analyses to validate the efficacy of our approach in mitigating cyber threats and enhancing network security.

2. RELATED WORK

In the realm of network intrusion detection, researchers have explored various methodologies to enhance detection accuracy and efficiency. An early work by Garcia-Teodoro et al. [30] delves into anomaly-based techniques, shedding light on the challenges and systems prevalent in network intrusion detection. Building upon this foundation, Catania and Garino [31] provide insights into automatic intrusion detection, discussing current techniques alongside open issues. In recent years, the integration of deep learning techniques has garnered significant attention. Niyaz et al. [32] and Javaid et al. [33] introduce deep learning approaches tailored for network intrusion detection, showcasing their efficacy in mitigating cyber threats. Furthermore, Vinayakumar et al. [9] leverage convolutional neural networks (CNNs) to bolster intrusion detection capabilities, demonstrating the applicability of advanced neural architectures in this domain. A comprehensive review by Samrin and Vasumathi [34] evaluates anomaly-based intrusion detection systems, offering a synthesized perspective on existing methodologies. Additionally, Shone et al. [35] propose a deep learning framework, emphasizing its potential for enhancing network security through intelligent intrusion detection mechanisms.

With the proliferation of Internet of Things (IoT) devices, Chaabouni et al. [36] address the unique challenges posed by IoT environments, advocating for learning-based intrusion detection techniques. Gamage and Samarabandu [24] further survey deep learning methods, providing an objective comparison to delineate their strengths and limitations. Ahmad et al. [25] conduct a systematic study on machine learning and deep learning approaches, elucidating their efficacy in network intrusion detection systems. Zhang et al. [26] offer a comparative analysis of various intrusion detection methods, facilitating an understanding of their relative performance and suitability. Recent advancements include hybrid models, as exemplified by Talukder et al. [27], who propose a dependable hybrid machine learning model tailored for intrusion detection. Moreover, Khafaga et al. [28] explore the synergy between ensemble classifiers and metaheuristic optimization, presenting a robust approach for network intrusion detection.

3. ALGORITHM AND MODEL

3.1 TabTransformer MODEL

As shown in Figure 1, the TabTransformer model is a powerful architecture designed for handling tabular data, including both categorical and numerical features. It combines the strengths of transformer-based architectures with innovative mechanisms tailored for tabular data processing. The TabTransformer model consists of two main components: the categorical transformer and the numerical transformer.

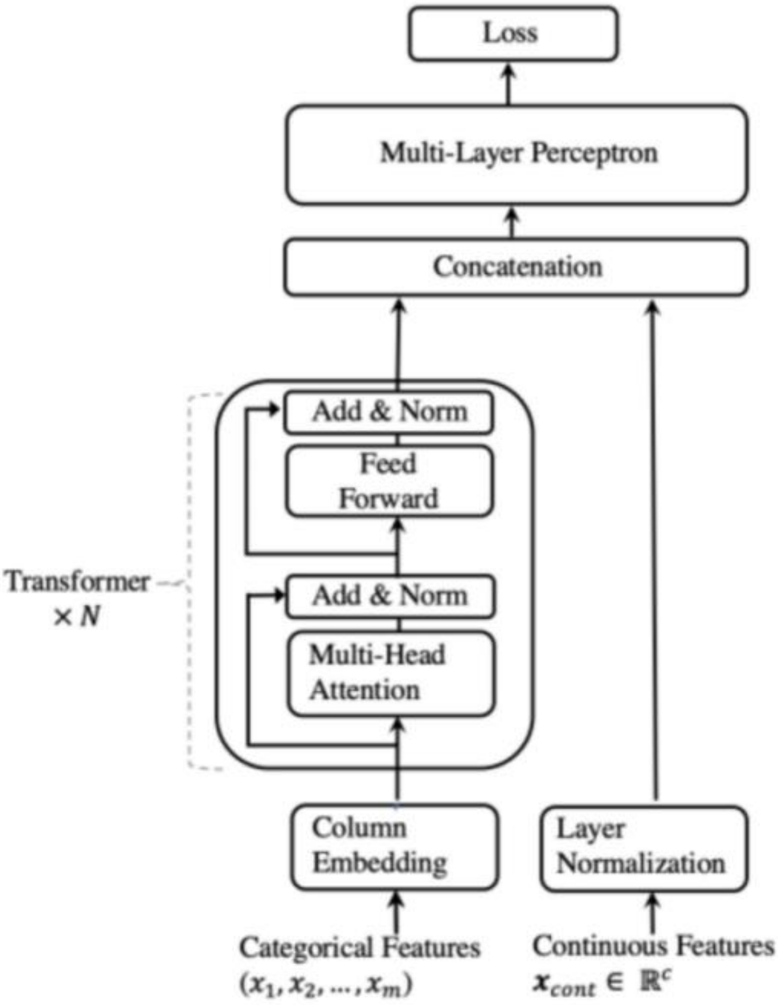

Figure 1: TabTransformer Model

In our model, the categorical transformer processes categorical features using embedding layers. Categorical features, denoted as E_{CATE}, such as 'protocol_type', 'service', and 'flag', are first transformed into dense embeddings using embedding layers. These embeddings capture the semantic relationships between different categories.

$$E_{CATE} = Column\_Embedding(x) \tag{1}$$

Furthermore, numerical transformer directly processes numerical features without additional transformation. Features like 'duration', 'src_bytes', and 'dst_bytes' are inputted into a sequence of fully connected layers, marked as E_{NUME}. These layers are designed to discern intricate patterns and correlations within the numerical feature domain. Layer normalization [37] is employed to extract features from numerical features.

$$E_{NUME} = Layer\_Normalization(x) \tag{2}$$

To ensure a comprehensive feature representation, we concatenate embeddings derived from both categorical and numerical features, amalgamating semantic relationships from categorical attributes and numerical patterns for a holistic portrayal of our feature set.

$$E_{concat} = Concatenate(E_{CATE}, E_{NUME}) \tag{3}$$

The combined embedding is subsequently forwarded through a binary classification layer, comprising fully connected layers and a softmax activation function. This layer computes probabilities for each class, distinguishing between "Normal" or "Anomalous" network connections.

$$P(recommendation = c|E_{concat}) = Softmax\big(FC(E_{concat})\big) \tag{4}$$

where c represents one of the classes ("Normal" or "Anomalous.").

By incorporating both categorical and numeric features and leveraging the power of the TabTransformer architecture, our proposed model offers a robust and effective solution for network intrusion detection. Through empirical validation and comparative analyses, we aim to demonstrate the efficacy and scalability of our approach in accurately identifying malicious activities and safeguarding network infrastructures against cyber threats.

3.2 Prospects of Large Language Models (LLM)

The integration of Large Language Models (LLMs), exemplified by GPT [38], GPT-2 [39], and GPT-3 [40], marks a significant advancement in the field of natural language understanding and processing. With their extensive pre-trained knowledge and contextual understanding of language [41-42], LLMs play a pivotal role in augmenting various applications, including network intrusion detection [43]. By harnessing the power of LLMs, network intrusion detection systems can benefit from enhanced contextual understanding of network traffic data and associated logs[44]. LLMs possess the ability to analyze and interpret vast amounts of textual information, such as financial information [45-46], segmentation [47-49] and classification [50-52], machinery [56], and vehicle localization [57-58] enabling them to identify and predict subtle patterns and anomalies indicative of malicious activities within network communications.

4. EXPERIMENTS

4.1 Datasets

The dataset under examination originates from a simulated military network environment, meticulously crafted to replicate the complexities of a typical US Air Force LAN. In this simulated environment, various intrusion scenarios were enacted, mirroring real-world cyber warfare situations. Each connection within the dataset represents a sequence of TCP packets exchanged between source and target IP addresses, adhering to predefined communication protocols. Notably, each connection is meticulously labeled as either "Normal" or "Anomalous," with the latter encompassing a diverse range of attack types. The dataset encapsulates a total of 41 features extracted from both normal and attack data, comprising a combination of qualitative and quantitative attributes. These features include indicators such as duration, bytes transferred, and various network protocol-related metrics. In total, the dataset encompasses 16,878 training samples, 2,826 validation samples, and 5,488 test samples, with a distribution ratio of 7:1:2 respectively. This balanced distribution enables robust model training and evaluation, facilitating the development of effective intrusion detection systems capable of accurately discerning between benign network traffic and malicious intrusions.

4.2 Evaluation metrics

Precision, Recall, and F1-score are the measures used in the named entity recognition. P (Positive) represents positive samples in all the samples. N (Negative) represents negative samples in all the samples. TP (True Positives) is the number of positive samples predicted as positive. FN (False Negatives) is the number of positive samples predicted as negative. FP (False Positives) is the number of negative samples predicted as positive. TN (True Negatives) is the number of negative samples predicted as negative. Precision is the proportion of true positive samples in all the samples that are predicted to be positive, which is defined as:

$$Precision = \frac{TP}{TP+FP} \tag{5}$$

Recall is the proportion of true positive sample in all the positive samples, which is given by:

$$Recall = \frac{TP}{TP+FN} \tag{6}$$

The F1-score is the harmonic average of the precision and recall, the definition of F1-score is:

$$F1 = \frac{2*Precison*Recall}{Precision+Recall} \tag{7}$$

4.3 Results

As shown in Table 1, here are the results obtained from different models evaluated in the study:

Table 1: Model Results

Model	Precision	Recall	F1-Score
SVM	95.69%	95.84%	95.77%
LR	94.16%	94.00%	94.08%
MLP	97.13%	95.92%	96.52%
Voting Model	95.53%	94.80%	95.17%
TabTransformer	98.87%	98.04%	98.45%

The table displays performance metrics for each evaluated model. SVM [53], LR [54], MLP [55], and the Voting Model exhibit commendable performance. However, TabTransformer surpasses them all, boasting the highest F1-score 98.45%. This underscores its superior effectiveness in network intrusion detection. TabTransformer's robust performance reaffirms its status as a leading choice for mitigating cyber threats and enhancing network security.

5. CONCLUSION

In conclusion, our study underscores the critical role of advanced machine learning models in network intrusion detection. Through comprehensive evaluation and comparison, we have identified TabTransformer as a standout performer, surpassing traditional models like SVM, LR, MLP, and a Voting Model in precision, recall, and F1-score metrics. TabTransformer's ability to effectively handle both categorical and numerical features, coupled with its capacity to capture intricate patterns within tabular data, positions it as a powerful tool for detecting and mitigating cyber threats in real-time. The implications of our findings are profound, especially in today's digital landscape where cyberattacks pose significant risks to organizations and individuals alike. By embracing innovative machine learning techniques like TabTransformer, stakeholders can bolster their defenses against evolving threats, safeguarding critical assets and infrastructure from potential breaches.

Furthermore, our study highlights the necessity of continuously advancing intrusion detection systems to keep pace with the ever-changing threat landscape. As cyber threats become increasingly sophisticated, the need for robust and adaptive defense mechanisms becomes more pressing. TabTransformer, with its superior performance and scalability, represents a promising solution for addressing these challenges and enhancing network security in an increasingly interconnected world.

REFERENCES

[1] Su, J., Nair, S., & Popokh, L. (2023, February). EdgeGYM: a reinforcement learning environment for constraint-aware NFV resource allocation. In 2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC) (pp. 1-7). IEEE.

[2] Popokh, L., Su, J., Nair, S., & Olinick, E. (2021, September). IllumiCore: Optimization Modeling and Implementation for Efficient VNF Placement. In 2021 International Conference on Software, Telecommunications and Computer Networks (SoftCOM) (pp. 1-7). IEEE.

[3] Jin, X., Manandhar, S., Kafle, K., Lin, Z., & Nadkarni, A. (2022, November). Understanding iot security from a market-scale perspective. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 1615-1629).

[4] Jin, X., Katsis, C., Sang, F., Sun, J., Bertino, E., Kompella, R. R., & Kundu, A. (2023). Prometheus: Infrastructure Security Posture Analysis with AI-generated Attack Graphs. arXiv preprint arXiv:2312.13119.

[5] Xiao, T., Xu, Z., He, W., Su, J., Zhang, Y., Opoku, R., ... & Jiang, Z. (2024). XTSFormer: Cross-Temporal-Scale Transformer for Irregular Time Event Prediction. arXiv preprint arXiv:2402.02258.

[6] Dang, B., Ma, D., Li, S., Dong, X., Zang, H., & Ding, R. (2024). Enhancing Kitchen Independence: Deep Learning-Based Object Detection for Visually Impaired Assistance. Academic Journal of Science and Technology, 9(2), 180–184.

[7] Jin, X., Pei, K., Won, J. Y., & Lin, Z. (2022, November). Symlm: Predicting function names in stripped binaries via context-sensitive execution-aware code embeddings. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 1631-1645).

[8] Li, H., Ding, D., & Zhang, J. (2020). Comprehensive Evaluation Model on New Product Introduction of Convenience Stores Based on Multidimensional Data. In Data Science: 6th International Conference, ICDS 2019, Ningbo, China, May 15–20, 2019, Revised Selected Papers 6 (pp. 40-50). Springer Singapore.

[9] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Applying convolutional neural network for network intrusion detection. In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1222-1228). IEEE.

[10] Luo, Y., Wei, Z., Xu, G., Li, Z., Xie, Y., & Yin, Y. (2024). Enhancing E-commerce Chatbots with Falcon-7B and 16-bit Full Quantization. Journal of Theory and Practice of Engineering Science, 4(02), 52-57.

[11] Su, J., Jiang, C., Jin, X., Qiao, Y., Xiao, T., Ma, H., ... & Lin, J. (2024). Large Language Models for Forecasting and Anomaly Detection: A Systematic Literature Review. arXiv preprint arXiv:2402.10350. Retrieved from http://arxiv.org/abs/2402.10350

[12] Liu, T., Xu, C., Qiao, Y., Jiang, C., & Chen, W. (2024). News Recommendation with Attention Mechanism. Journal of Industrial Engineering and Applied Science, 2(1), 21-26.

[13] Ji, H., Xu, X., Su, G., Wang, J., & Wang, Y. (2024). Utilizing Machine Learning for Precise Audience Targeting in Data Science and Targeted Advertising. Academic Journal of Science and Technology, 9(2), 215-220.

[14] Wang, X., Xiao, T., & Shao, J. (2021). EMRM: Enhanced Multi-source Review-Based Model for Rating Prediction. In Knowledge Science, Engineering and Management: 14th International Conference, KSEM 2021, Tokyo, Japan, August 14–16, 2021, Proceedings, Part III 14 (pp. 487-499). Springer International Publishing.

[15] Jing, Z., Su, Y., Han, Y., Yuan, B., Liu, C., Xu, H., & Chen, K. (2024). When Large Language Models Meet Vector Databases: A Survey. arXiv preprint arXiv:2402.01763.

[16] He, Z., Chen, W., Zhou, Y., Weng, H., & Shen, X. (2023). The Importance of AI Algorithm Combined With Tunable LCST Smart Polymers in Biomedical Applications. Frontiers in Computing and Intelligent Systems, 6(3), 92-95.

[17] Bao, W., Che, H., & Zhang, J. (2020, December). Will_Go at SemEval-2020 Task 3: An accurate model for predicting the (graded) effect of context in word similarity based on BERT. In Proceedings of the Fourteenth Workshop on Semantic Evaluation (pp. 301-306).

[18] Xie, Y., Li, Z., Yin, Y., Wei, Z., Xu, G., & Luo, Y. (2024). Advancing Legal Citation Text Classification A Conv1D-Based Approach for Multi-Class Classification. Journal of Theory and Practice of Engineering Science, 4(02), 15-22.

[19] Xu, X., Yuan, B., Song, T., & Li, S. (2023, November). Curriculum Recommendations Using Transformer Base Model with InfoNCE Loss And Language Switching Method. In 2023 5th International Conference on Artificial Intelligence and Computer Applications (ICAICA) (pp. 389-393). IEEE.

[20] Jin, X., Larson, J., Yang, W., & Lin, Z. (2023). Binary Code Summarization: Benchmarking ChatGPT/GPT-4 and Other Large Language Models. arXiv preprint arXiv:2312.09601.

[21] Song, X., Wu, D., Zhang, B., Peng, Z., Dang, B., Pan, F., & Wu, Z. (2023). ZeroPrompt: Streaming Acoustic Encoders are Zero-Shot Masked LMs. INTERSPEECH 2023, 1648–1652.

[22] Liu, Y., Yang, H., & Wu, C. (2023). Unveiling patterns: A study on semi-supervised classification of strip surface defects. IEEE Access, 11, 119933-119946.

[23] Su, J., Nair, S., & Popokh, L. (2022, November). Optimal resource allocation in sdn/nfv-enabled networks via deep reinforcement learning. In 2022 IEEE Ninth International Conference on Communications and Networking (ComNet) (pp. 1-7). IEEE.

[24] Gamage, S., & Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. Journal of Network and Computer Applications, 169, 102767.

[25] Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150.

[26] Zhang, C., Jia, D., Wang, L., Wang, W., Liu, F., & Yang, A. (2022). Comparative research on network intrusion detection methods based on machine learning. Computers & Security, 121, 102861.

[27] Talukder, M. A., Hasan, K. F., Islam, M. M., Uddin, M. A., Akhter, A., Yousuf, M. A., ... & Moni, M. A. (2023). A dependable hybrid machine learning model for network intrusion detection. Journal of Information Security and Applications, 72, 103405.

[28] Khafaga, D. S., Karim, F. K., Abdelhamid, A. A., El-kenawy, E. S. M., Alkahtani, H. K., Khodadadi, N., ... & Ibrahim, A. (2023). Voting Classifier and Metaheuristic Optimization for Network Intrusion Detection. Computers, Materials & Continua, 74(2).

[29] Huang, X., Khetan, A., Cvitkovic, M., & Karnin, Z. (2020). Tabtransformer: Tabular data modeling using contextual embeddings. arXiv preprint arXiv:2012.06678.

[30] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. computers & security, 28(1-2), 18-28.

[31] Catania, C. A., & Garino, C. G. (2012). Automatic network intrusion detection: Current techniques and open issues. Computers & Electrical Engineering, 38(5), 1062-1072.

[32] Niyaz, Q., Sun, W., Javaid, A. Y., & Alam, M. (2015, December). A deep learning approach for network intrusion detection system. In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (Formerly BIONETICS), BICT-15 (Vol. 15, No. 2015, pp. 21-26).

[33] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016, May). A deep learning approach for network intrusion detection system. In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS) (pp. 21-26).

[34] Samrin, R., & Vasumathi, D. (2017, December). Review on anomaly based network intrusion detection system. In 2017 international conference on electrical, electronics, communication, computer, and optimization techniques (ICEECCOT) (pp. 141-147). IEEE.

[35] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE transactions on emerging topics in computational intelligence, 2(1), 41-50.

[36] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.

[37] Ba, J. L., Kiros, J. R., & Hinton, G. E. (2016). Layer normalization. arXiv preprint arXiv:1607.06450.

[38] Radford, A., Narasimhan, K., Salimans, T., & Sutskever, I. (2018). Improving language understanding by generative pre-training.

[39] Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., & Sutskever, I. (2019). Language models are unsupervised multitask learners. OpenAI blog, 1(8), 9.

[40] Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J. D., Dhariwal, P., ... & Amodei, D. (2020). Language models are few-shot learners. Advances in neural information processing systems, 33, 1877-1901.

[41] Xiong, J., Feng, M., Wang, X., Jiang, C., Zhang, N., & Zhao, Z. (2024). Decoding sentiments: Enhancing covid-19 tweet analysis through bert-rcnn fusion. Journal of Theory and Practice of Engineering Science, 4(01), 86-93.

[42] Zhao, Z., Zhang, N., Xiong, J., Feng, M., Jiang, C., & Wang, X. (2024). Enhancing E-commerce Recommendations: Unveiling Insights from Customer Reviews with BERTFusionDNN. Journal of Theory and Practice of Engineering Science, 4(02), 38-44.

[43] Su, Jing, et al. "Large Language Models for Forecasting and Anomaly Detection: A Systematic Literature Review." arXiv preprint arXiv:2402.10350 (2024).

[44] Chen, W., Shen, Z., Pan, Y., Tan, K., & Wang, C. (2024). Applying Machine Learning Algorithm to Optimize Personalized Education Recommendation System. Journal of Theory and Practice of Engineering Science, 4(01), 101-108.

[45] Qiao, Y., Jin, J., Ni, F., Yu, J., & Chen, W. (2023). Application of machine learning in financial risk early warning and regional prevention and control: A systematic analysis based on shap. WORLD TRENDS, REALITIES AND ACCOMPANYING PROBLEMS OF DEVELOPMENT, 331.

[46] Liu, S., Wu, K., Jiang, C., Huang, B., & Ma, D. (2023). Financial time-series forecasting: Towards synergizing performance and interpretability within a hybrid machine learning approach. arXiv preprint arXiv:2401.00534.

[47] Dang, B., Ma, D., Li, S., Dong, X., Zang, H., & Ding, R. (2024). Enhancing Kitchen Independence: Deep Learning-Based Object Detection for Visually Impaired Assistance. Academic Journal of Science and Technology, 9(2), 180–184.

[48] Ma, D., Dang, B., Li, S., Zang, H., & Dong, X. (2023). Implementation of computer vision technology based on artificial intelligence for medical image analysis. International Journal of Computer Science and Information Technology, 1(1), 69–76.

[49] Qiao, Y., Ni, F., Xia, T., Chen, W., & Xiong, J. (2024, January). Automatic recognition of static phenomena in retouched images: A novel approach. In The 1st International scientific and practical conference “Advanced technologies for the implementation of new ideas”(January 09-12, 2024) Brussels, Belgium. International Science Group. 2024. 349 p. (p. 287).

[50] Li, S., Kou, P., Ma, M., Yang, H., Huang, S., & Yang, Z. (2024). Application of Semi-supervised Learning in Image Classification: Research on Fusion of Labeled and Unlabeled Data. IEEE Access.

[51] Niu, H., Li, H., Wang, J., Xu, X., & Ji, H. (2023). Enhancing computer digital signal processing through the utilization of rnn sequence algorithms. International Journal of Computer Science and Information Technology, 1(1), 60-68.

[52] Wang, X., Xiao, T., Tan, J., Ouyang, D., & Shao, J. (2020). MRMRP: multi-source review-based model for rating prediction. In Database Systems for Advanced Applications: 25th International Conference, DASFAA 2020, Jeju, South Korea, September 24–27, 2020, Proceedings, Part II 25 (pp. 20-35). Springer International Publishing.

[53] Vishwanathan, S. V. M., & Murty, M. N. (2002, May). SSVM: a simple SVM algorithm. In Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No. 02CH37290) (Vol. 3, pp. 2393-2398). IEEE.

[54] Maulud, D., & Abdulazeez, A. M. (2020). A review on linear regression comprehensive in machine learning. Journal of Applied Science and Technology Trends, 1(2), 140-147.

[55] Taud, H., & Mas, J. F. (2018). Multilayer perceptron (MLP). Geomatic approaches for modeling land change scenarios, 451-455.

[56] Ni, F., Zang, H., & Qiao, Y. (2024, January). Smartfix: Leveraging machine learning for proactive equipment maintenance in industry 4.0. In The 2nd International scientific and practical conference “Innovations in education: prospects and challenges of today”(January 16-19, 2024) Sofia, Bulgaria. International Science Group. 2024. 389 p. (p. 313).

[57] Liu, T., Xu, C., Qiao, Y., Jiang, C., & Yu, J. (2024). Particle Filter SLAM for Vehicle Localization. Journal of Industrial Engineering and Applied Science, 2(1), 27-31.

[58] Dai, J., Dai, S., Wang, J., Luo, Z., & Zhu, N. (2024). On the Current Status and Trends of Short Video Self Media Development in the 5G Era. Academic Journal of Sociology and Management, 2(2), 5-9.