International Journal of Computer Science and Information Technology
ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 2, Number 1, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v2n1.37
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Intelligent Security Detection and Defense in Operating Systems Based on Deep Learning

Hongbo Wang[1,*], Jiang Wu[2], Chenwei Zhang[3], Wenran Lu[4], Chunhe Ni[5]

[1]Computer Science, University of Southern California, Los Angeles, CA, USA

[2]Computer Science, University of Southern California, Los Angeles, CA, USA

[3]Electrical and Computer Engineering, University of Illinois Urbana-Champaign, Urbana, IL, USA

[4]Electrical Engineering, University of Texas at Austin, Austin, TX, USA

[5]Computer Science, University of Texas at Dallas, Richardson, TX, USA

*Corresponding Author: hongbowa@usc.edu

ABSTRACT

With the development of network technology, APT(advanced persistentthreat) attacks are increasing, and research on the security of enterprise assets requires effective detection of digital assets in the network space and effective management of assets through screening and combing, which is the key to real-time monitoring of the safe operation of the system. However, the accompanying malware also poses a threat to the user's property and privacy, so an effective method of detecting Android malware is necessary. In this research direction, although the feature processing capability of traditional machine learning has been improved, there are problems that feature extraction relies on expert experience and the accuracy is low. Therefore, this paper combines deep learning reinforcement technology with the operating system to detect and defend the system in advance, so as to achieve network security.

KEYWORDS

Operating system; Network security; Deep learning; Enhance

1. INTRODUCTION

With the rapid development of science and technology, mobile devices have gained rapid popularity and become a part of People's Daily life. The portability and portability of mobile devices has revolutionized the communications and entertainment industries. According to a report by Statista, the number of mobile devices used is growing every year. The report shows that worldwide, the number of users of mobile smart devices has reached 6.3 billion by 2021, an increase of 75% in a fairly short period of five years.[3] In addition, a report published by Statista suggests that the number of smartphone users could reach 7.3 billion by 2025, which is more than half of the world's population [4]. The Android operating system is popular for the following reasons :1. Open system. GooglePlay comes standard with almost all smartphones and tablets so that users can find and download new software, but unlike other companies, Google gives users the option to install apps from third-party app stores. Users can download apps directly from developer sites, install them from flash cards or third-party app stores. 2. Customize the user interface. Google has been working hard to make the user interface (UI) of Android phones as flexible and customizable as possible, to this end, Google has loaded Android phones with a series of customizable widgets that can be used anywhere in the UI, [5]providing updates or shortcuts to various services, such as email, calendar, and messages. 3.

Open source code. The Android operating system allows developers and hardware manufacturers to make changes to the core software of the operating system, which allows companies to make changes to the operating system to work in specific industries; 4. Innovation market is faster. The Android platform has a strong track record of supporting the latest cutting-edge ideas. While casual apps still seem to be on almost every operating system at the same time, the bigger hardware innovations almost all started with Google 5. Custom ROM. [6]There are a lot of third-party apps that provide users with advanced features of Android, and one of the best things is that people can use it, modify all of its features, and install a custom version instead of the one that came with your phone. It will allow you to make many system-level adjustments that are not easily possible on any other operating system, such as Windows or IOS.

Therefore, through the operation of the computer system, it is possible to share the massive information resources stored in the network and system, pass some useful and valuable information to the users, and further optimize the resources, which is obvious to all industries and fields to improve work efficiency and the role and effect of industry development and progress. And all the time, the security of computer operating system is also like a shadow, which poses a threat to the computer operation effect. [7-10]Therefore, it is particularly important and urgent to discuss the construction of multi-dimensional security maintenance framework of computer operating system based on the analysis of computer system security problems.

2. RELATED WORK

Computer operating system design companies will continue to carry out in-depth research and development and upgrade of the issued operating system, they regularly update the security vulnerabilities of some systems, and release them to users in a certain way.[11] Users can improve the security of the operating system to some extent by maintaining and updating the security holes of the operating system in time.

2.1. Deep Learning for Malware Detection

In a signature-based static detection and classification approach, FengY et al. combine static blemish analysis with a new form of procedural representation of intercomponent call graphs for signature matching algorithms to effectively detect Android applications with certain control and data flow characteristics. In the static detection and classification method based on Dalvik bytecode, [12]Li Ting et al. cut the program according to DEX format to get instruction blocks in method unit. Then the feature is generated by Dalvik instruction in the block, and the similarity between the feature and known malware is calculated by distance algorithm and similarity measurement algorithm, and the existence of malicious code is judged according to the similarity. [13]Grace M et al. analyze the Dalvik bytecode to determine whether a particular application is exhibiting dangerous behavior (for example, launching a root exploit or sending a background SMS message), and the output is then used to generate a prioritized list of reduced applications.

The detection and classification method of Android malware based on network-level features refers to the characteristic analysis method of network traffic generated by the software in the actual running process. According to the subsequent processing methods of features, currently, dynamic analysis methods based on network level features are mainly divided into two categories - detection and classification methods of Android malware based on machine learning and deep learning.

In the Android malware detection and classification method based on machine learning, by designing the Android malware traffic behavior monitoring method, the traffic data generated by 5560 malware samples in the actual network environment is captured in the first 5 minutes, and by analyzing these traffic data, Three conclusions were drawn :[14-18](1) More than 70% of malware generated malicious traffic within the first 5 minutes; (2)DNS queries and HTTP requests can be used to identify

malware, and the detection rate is 69.55% and 40.89%, respectively; (3) Adware traffic data can greatly affect malware detection. This provides the research direction for the later researchers in related fields. Some researchers also extracted 22 traffic features, and then identified malware according to different combinations of 22 features, and found that one of the combinations including specific 9 features achieved the best identification effect.[19] LashkariAH uses CICFlowMeter to extract 17 dynamic traffic characteristics from network traffic, and then filters through it, and finally uses 9 dynamic traffic characteristics including maximum packet length, minimum packet length of stream, reverse variance data bytes, etc., for malware detection. In each defined period of time, ShabtaiA extracts (that is, measures and captures) the statistical characteristics of the mean value, standard deviation, [20]minimum value and maximum value (in bytes) of the sent and received data for each running application, and then learns and trains these statistical characteristics through machine learning to establish the standard of various statistical characteristics of benign software. This method shows that statistical features can represent the behavior of malware and thus identify malware.

2.2. Advantages of deep learning over traditional signature-based methods

1. Detection of Previously Unknown Threats: Deep learning models can detect previously unseen malware or threats by learning patterns and behaviors from large datasets. Unlike signature-based methods, which rely on known patterns, deep learning algorithms can identify novel threats based on similarities with known malicious behavior. For example, in a study conducted by researchers at Endgame, deep learning-based models were able to detect malware variants that were not present in signature databases, showcasing the effectiveness of this approach.

2. Reduced False Positives:Deep learning models can significantly reduce false positives compared to signature-based methods. By analyzing multiple aspects of a file or network traffic, deep learning algorithms can make more accurate decisions about whether a file or activity is malicious. This leads to fewer false alarms and reduces the burden on security teams. For instance, a case study by Cylance demonstrated that their deep learning-based antivirus solution had a significantly lower false positive rate compared to traditional signature-based antivirus software.

3. Adaptability to Evolving Threats:Deep learning models can adapt to evolving threats without requiring frequent updates to signature databases. Traditional signature-based methods often struggle to keep up with the rapid pace of malware evolution, requiring constant updates to detect new threats. In contrast, deep learning models can continuously learn from new data and adapt their detection capabilities accordingly. For example, a study by Microsoft Research showed that deep learning models were effective in detecting polymorphic malware variants that change their appearance to evade detection.

4. [21]Detection of Advanced Persistent Threats (APTs): Deep learning models are more effective at detecting advanced persistent threats (APTs) and sophisticated attacks that may not exhibit obvious patterns or signatures. These attacks often involve multiple stages and use advanced evasion techniques to avoid detection by traditional methods. Deep learning algorithms excel at identifying subtle anomalies and behavioral patterns that may indicate the presence of an APT. For instance, a case study by Darktrace demonstrated how their deep learning-based cybersecurity platform successfully detected APTs that evaded traditional security measures.

Overall, deep learning offers several advantages over traditional signature-based methods in cybersecurity, including the ability to detect unknown threats, reduce false positives, adapt to evolving threats, and detect advanced persistent threats more effectively. These advantages have been demonstrated in various real-world studies and case examples, highlighting the potential of deep learning in enhancing cybersecurity defenses.

2.3. Examples of successful malware detection using deep learning

2.3.1. Endgame's Deep Learning Model:

Endgame, a cybersecurity company, developed a deep learning-based malware detection model capable of detecting previously unseen threats.

In a study, Endgame's model successfully detected malware variants that were not present in signature databases, showcasing its ability to identify novel threats.

The model's performance was evaluated using real-world datasets, demonstrating its effectiveness in detecting previously unknown malware with high accuracy.

2.3.2. Cylance's Antivirus Solution:

Cylance, an AI-driven cybersecurity company, developed an antivirus solution based on deep learning algorithms.

In a case study, Cylance's solution demonstrated a significantly lower false positive rate compared to traditional signature-based antivirus software.

By analyzing file attributes and behavior patterns, the deep learning model accurately identified malware while minimizing false alarms.

2.3.3. Microsoft Research's Study on Polymorphic Malware:

Researchers at Microsoft Research conducted a study on detecting polymorphic malware variants using deep learning.The study showed that deep learning models were effective in detecting malware variants that change their appearance to evade detection.By learning from a large dataset of malware samples, the deep learning models were able to generalize and detect previously unseen variants with high accuracy.

2.3.4. Darktrace's Cybersecurity Platform:

Darktrace, an [22]AI-powered cybersecurity company, developed a platform based on unsupervised deep learning algorithms.

In various case studies, Darktrace's platform successfully detected advanced persistent threats (APTs) and sophisticated attacks that evaded traditional security measures.By analyzing network traffic and user behavior in real-time, the deep learning algorithms identified subtle anomalies indicative of APTs, enabling proactive threat detection and response.

These case studies and examples highlight the effectiveness of deep learning in malware detection, particularly in detecting unknown threats, reducing false positives, and detecting advanced and polymorphic malware variants. The success of these approaches demonstrates the potential of deep learning to enhance cybersecurity defenses and protect against evolving threats.

In conclusion, the multi-dimensional security maintenance framework of computer operating system based on deep learning not only breaks the one-to-one mode of defense measures and attack schemes, but also fends off undiscovered attacks. [23-24]Compared with the traditional defense scheme, it also has the characteristics of strong versatility and good deployability, and is a new security maintenance strategy, which is of great significance for the construction of secure and trusted operating system. The security maintenance of computer network is of great importance, and all staff should understand the multidimensional security maintenance framework of computer operating system based on deep learning, improve security network technology, pay attention to the application of network security technology, scientific management and effective use, improve the security factor of computer network, and build a safe and controllable network environment.

3. METHODOLOGY

Mimicry in the biological world refers to the simulation of shape. A creature simulates another creature in terms of movement, shape and other characteristics, so as to avoid natural enemies and dangers, confuse the line of sight of attackers, and thus play a role in defending against attacks. In this way, one or both parties can benefit, and this is a defense that organisms have developed over the long course of evolution. Inspired by the camouflage defense based on mimicry, the concept of mimicry defense came into being.

3.1. Dynamic heterogeneous redundant architecture

Dynamic Heterogeneous Redundancy (DHR) architecture has significant advantages in operating system security detection. First, it uses multiple layers of security protection, including redundancy at the hardware, operating system, and application levels, so that attackers need to overcome multiple obstacles to successfully penetrate the system. This multi-level protection can improve the overall security of the system and reduce the possibility of exploiting security vulnerabilities.

Second, DHR architecture has the ability to respond in real time. It can monitor the status of the system in real time and take corresponding defensive measures according to the detected threat intelligence. This real-time response capability enables the system to respond to emerging threats in a timely manner and protect the system from attacks.

In addition, DHR architecture can also integrate deep learning technology, [25]using its powerful data analysis and pattern recognition capabilities to enhance the effectiveness of security detection. Deep learning models can continuously learn and adapt to new threat patterns while monitoring system status in real time, improving the accuracy and intelligence of detection. DHR architecture uses an adaptive defense mechanism to dynamically adjust security policies according to system operating status and detected threat intelligence. This adaptability enables the system to respond in time to the ever-changing threat environment and maintain security and stability.

Finally, DHR architecture realizes efficient security detection and defense by optimizing resource utilization. The design of dynamic heterogeneous redundancy enables the system to flexibly allocate resources, improve the coverage and efficiency of security protection according to actual needs, and minimize resource waste. In summary, dynamic heterogeneous redundant architecture has obvious advantages in operating system security detection, and provides important support for building comprehensive, intelligent and efficient security protection.

3.2. Recurrent neural network

In the late 20th century, the Recurrent Neural Network (RNN) was introduced by Elman and Jordan, among others, which became pivotal for the subsequent advancements in deep learning. RNNs are specialized neural network architectures adept at handling sequential data, and they have found widespread applications in various fields, including handwriting recognition and speech recognition. [26]At its core, an RNN establishes connections between its cell units in a directed cycle, enabling it to retain memory of previous data information through its internal cell state. This allows the network to maintain contextual understanding and capture temporal dependencies within sequential data. Specifically, the output information of the RNN at time step $t-1$ can directly influence the input information of the RNN at time step t, facilitating the modeling of sequential patterns and dynamics.

The inherent ability of RNNs to capture temporal dependencies makes them well-suited for tasks involving time series data, natural language processing, and other sequential data processing tasks. By leveraging the recurrent connections and memory capabilities, RNNs have become an

indispensable tool in various deep learning applications, enabling more effective modeling and prediction of sequential data.

One of the key factors of security of mimicry architecture is that it has multiple functionally equivalent heterogeneous redundant bodies. As a system function responding to external service requests, only heterogeneous redundant bodies can avoid being attacked by attackers. [27]At the same time, "heterogeneous" is the basis of functionally equivalent heterogeneous redundant bodies, which can avoid attackers' ability to sniff and exploit system vulnerabilities. Therefore, we must study the execution body set, so that when scheduling multiple execution bodies in the functionally equivalent execution body set to respond to external service requests, we can find the scheduling basis to achieve the optimal scheduling, and fundamentally ensure the security of the whole mimicry architecture.

3.3. LSTM

The concept of Long Short-Term Memory (LSTM) was proposed by Hochreiter and Schmidhuber et al. Compared with the traditional recurrent neural network, LSTM network is a new structure, which introduces the memory unit. Each memory unit contains four main elements: input gate i, forgetting gate f, output gate o, and neuronal self-circulation. These gates allow cells to store and access information for a long time. The input gate i of the LSTM controls the input of the LSTM hidden unit, the forgetting gate f determines the data amount flowing through the LSTM hidden unit, and the output gate o controls the output result of the LSTM hidden unit. Three gating systems and the cell status value c enable the LSTM to better learn to serialize data. LSTM easily remembers correlations between short - and long-term input data, and is able to overcome problems of disappearing gradients and exploding gradients.

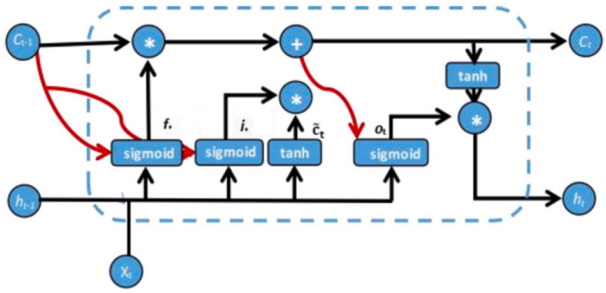

Figure 1. Hidden unit structure of LSTM

Long Short-Term Memory network (LSTM) can play an important role in the security detection of operating system. LSTM is a special type of recurrent neural network (RNN) with powerful memory, which can efficiently process sequence data and retain long-term dependencies in time. In terms of security detection, [28]LSTM can be used to detect various types of malicious behavior, such as abnormal network traffic, malware behavior, and intrusion attempts.

The basic principles of LSTM for operating system security detection are as follows:

1. Sequence modeling: LSTM can serialize various activities in the operating system, such as system call sequence, network traffic sequence, etc. By feeding these sequences into the LSTM model, the behavior patterns of the system can be modeled and learned.

2. Long-term dependency: LSTM can effectively capture long-term dependency in sequence data through its gating mechanism (such as input gate, forget gate and output gate). This means that the LSTM can remember past behavior to better understand the current state of the system and make predictions.

3. Anomaly detection: During the training phase, LSTM can learn patterns of normal system behavior. In the event of abnormal behavior, such as an abnormal sequence of system calls or abnormal network traffic patterns, the LSTM will be able to detect and issue an alert.

4. Real-time monitoring: The LSTM model deployed in the operating system can monitor the behavior of the system in real time and identify abnormal behavior according to pre-trained patterns. In this way, potential security threats can be discovered in time and corresponding countermeasures can be taken.

A common application is to use LSTM to detect network intrusion behavior. [29]By inputting network traffic data into the LSTM model for training, the model can learn normal network traffic patterns. In the event of abnormal network traffic behavior, such as a large-scale DDoS attack or unauthorized access behavior, LSTM will be able to identify these abnormal behaviors and issue alerts to help network administrators take timely measures to protect the security of the system. Another example is the use of LSTM to detect malware behavior. By modeling and training the behavior sequence of the malware, LSTM can learn the characteristic patterns of the malware and find similar behaviors in the system. Once malware activity is detected, LSTM will be able to identify and deal with it in a timely manner, preventing it from causing more damage.

These practical cases demonstrate the potential of LSTM in operating system security detection. Through sequence modeling and long-term dependency capture, LSTM can help improve the accuracy and efficiency of security detection and protect the system from various security threats.

3.4. Dynamic detection structure of mimicry Android malware based on enhanced deep learning

Based on the principle of non-similar redundancy architecture in mimicry security, a dynamic detection structure of mimicry Android malware based on enhanced deep learning is proposed. When mimicry architecture is applied to Android malware detection, the actuators in the execution body set (A1,A2,.an) in the non-similar redundancy construction are all Android malware detection algorithms. For example, A1 is the dynamic detection algorithm of Android malware based on LSTM model. [30]A2 is a dynamic detection algorithm of Android malware based on GRU model. A3 is a dynamic detection algorithm of Android malware based on capsule network model. A4 is another deep learning algorithm for the dynamic detection of Android malware. Three enhanced deep learning algorithms, namely enhanced LSTM algorithm, enhanced GRU algorithm and enhanced capsule network algorithm, are selected in the proposed enhanced deep learn-based mimicry Android malware dynamic detection structure. These three algorithms serve as three independent actuators of the dynamic detection structure of mimicry Android malware enhanced by deep learning.

Compared with traditional deep learning algorithms, the enhanced LSTM algorithm, the enhanced GRU algorithm and the enhanced capsule network algorithm can learn the historical information features of the input data better, and have a better ability to learn the long distance features. [31]The enhanced LSTM algorithm, the enhanced GRU algorithm and the enhanced capsule network algorithm are selected as the three executor sets of the simulated Android malware dynamic detection structure of enhanced deep learning to ensure that the input data can be more accurate in the dynamic detection of Android malware no matter which executor set is selected.

4. CONCLUSION

In conclusion, the integration of deep learning techniques with dynamic security architectures presents a promising approach to enhance the security of computer operating systems and mitigate cyber threats effectively. By leveraging the capabilities of dynamic heterogeneous redundancy architecture and advanced deep learning models such as recurrent neural networks (RNNs) and Long Short-Term Memory (LSTM), the system can detect and respond to various security risks in real-time. This approach offers multiple layers of security protection, real-time threat response capabilities, and efficient resource utilization, contributing to a comprehensive and robust security maintenance framework for computer operating systems. Moreover, the proposed dynamic detection structure of

mimicry Android malware based on enhanced deep learning demonstrates the effectiveness of advanced deep learning algorithms in improving the accuracy and efficiency of malware detection, further strengthening the security posture of computer systems.

ACKNOWLEDGEMENT

We would like to thank Zhou Yanlin et al for their article in the Journal of Theory and Practice of Engineering Science, It is entitled Utilizing AI-Enhanced Multi-Omics Integration for Predictive Modeling of Disease Susceptibility in Functional Organization Phenotypes. Their work has made important contributions to predictive modeling of disease susceptibility in functional phenotypes using AI-enhanced multi-omics integration. In addition, they promote interdisciplinary research. Their work not only provides a novel way to integrate multi-omics data, it also opens up new avenues for predictive modeling of disease susceptibility in functional phenotypes. This research has important implications for understanding the pathogenesis and individual susceptibility of complex diseases, and provides new ideas and possibilities for future disease prevention and personalized medicine. Their efforts have made valuable contributions to research at the intersection of medicine, biology, and artificial intelligence, advancing the development of integrated sexual health research.

REFERENCES

[1] K. Xu, X. Wang, Z. Hu and Z. Zhang, "3D Face Recognition Based on Twin Neural Network Combining Deep Map and Texture," 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 2019, pp. 1665-1668, doi: 10.1109/ICCT46805.2019.8947113.

[2] Zhenghua Hu, Xianmei Wang, Kangming Xu, and Pu Dong. 2020. Real-time Target Tracking Based on PCANet-CSK Algorithm. In Proceedings of the 2019 3rd International Conference on Computer Science and Artificial Intelligence (CSAI '19). Association for Computing Machinery, New York, NY, USA, 343–346. https://doi.org/10.1145/3374587.3374607.

[3] Shi, Peng, Yulin Cui, Kangming Xu, Mingmei Zhang, and Lianhong Ding. 2019. "Data Consistency Theory and Case Study for Scientific Big Data" Information 10, no. 4: 137. https://doi.org/10.3390/info10040137.

[4] Wang, G., Gong, Y., Zhu, M., Yuan, J., & Wei, K. (2023). Unveiling the future navigating next-generation ai frontiers and innovations in application. International Journal of Computer Science and Information Technology, 1(1), 147-156.

[5] Ji, Huan, et al. "Utilizing Machine Learning for Precise Audience Targeting in Data Science and Targeted Advertis ing." Academic Journal of Science and Technology 9.2 (2024): 215-220.

[6] Qian, Wenpin, et al. "Clinical Medical Detection and Diagnosis Technology Based on the AlexNet Network Mode l." Academic Journal of Science and Technology 9.2 (2024): 207-211.

[7] Wu, Jiang, et al. "Case Study of Next-Generation Artificial Intelligence in Medical Image Diagnosis Based on Cloud Computing." Journal of Theory and Practice of Engineering Science 4.02 (2024): 66-73.

[8] Zhu, Mingwei, et al. "Enhancing Collaborative Machine Learning for Security and Privacy in Federated Learning. " Journal of Theory and Practice of Engineering Science 4.02 (2024): 74-82.

[9] Yang, Le, et al. "Research and Application of Visual Object Recognition System Based on Deep Learning and Ne ural Morphological Computation." International Journal of Computer Science and Information Technology 2.1 (20 24): 10-17.

[10] Chen, Jianhang, et al. "One-stage object referring with gaze estimation." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022.

[11] Qian, Jili, et al. "A Liver Cancer Question-Answering System Based on Next-Generation Intelligence and the Large Model Med-PaLM 2." International Journal of Computer Science and Information Technology 2.1 (2024): 28-35.

[12] Duan, Shiheng, et al. “Prediction of Atmospheric Carbon Dioxide Radiative Transfer Model Based on Machine Le arning”. Frontiers in Computing and Intelligent Systems, vol. 6, no. 3, Jan. 2024, pp. 132-6, https://doi.org/10.54097/ObMPjw5n.

[13] Chen , Jianfeng, et al. “Implementation of an AI-Based MRD Evaluation and Prediction Model for Multiple Myeloma”. Frontiers in Computing and Intelligent Systems, vol. 6, no. 3, Jan. 2024, pp. 127-31, https://doi.org/10.54097/zJ4MnbWW.

[14] “Machine Learning Model Training and Practice: A Study on Constructing a Novel Drug Detection System”. International Journal of Computer Science and Information Technology, vol. 1, no. 1, Dec. 2023, pp. 139-46, https://doi.org/10.62051/ijcsit.v1n1.19.

[15] Zhang, Y., & Zhang, H. (2023). Enhancing robot path planning through a twin-reinforced chimp optimization algorithm and evolutionary programming algorithm. IEEE Access.

[16] Shen, Zepeng, et al. "EDUCATIONAL INNOVATION IN THE DIGITAL AGE: THE ROLE AND IMPACT OF NLP TECHNOLOGY." OLD AND NEW TECHNOLOGIES OF LEARNING DEVELOPMENT IN MODERN CONDITIONS (2024): 281.

[17] Gong, Yulu, et al. "RESEARCH ON A MULTILEVEL PRACTICAL TEACHING SYSTEM FOR THE COURSE'DIGITAL IMAGE PROCESSING." OLD AND NEW TECHNOLOGIES OF LEARNING DEVELOPMENT IN MODERN CONDITIONS (2024): 272.

[18] Zhang, Y., Abdullah, S., Ullah, I., & Ghani, F. (2024). A new approach to neural network via double hierarchy linguistic information: Application in robot selection. Engineering Applications of Artificial Intelligence, 129, 107581.

[19] Qian, Wenpin, et al. "NEXT-GENERATION ARTIFICIAL INTELLIGENCE INNOVATIVE APPLICATIONS OF LARGE LANGUAGE MODELS AND NEW METHODS." OLD AND NEW TECHNOLOGIES OF LEARNING DEVELOPMENT IN MODERN CONDITIONS (2024): 262.

[20] W. Sun, W. Wan, L. Pan, J. Xu, and Q. Zeng, “The Integration of Large-Scale Language Models Into Intelligent Adjudication: Justification Rules and Implementation Pathways”, Journal of Industrial Engineering & Applied Science, vol. 2, no. 1, pp. 13–20, Feb. 2024.

[21] Zhou, Yanlin, et al. "Utilizing AI-Enhanced Multi-Omics Integration for Predictive Modeling of Disease Susceptibility in Functional Phenotypes." Journal of Theory and Practice of Engineering Science 4.02 (2024): 45-51.

[22] Liang, Penghao, et al. "Enhancing Security in DevOps by Integrating Artificial Intelligence and Machine Learning." Journal of Theory and Practice of Engineering Science 4.02 (2024): 31-37.

[23] Zhang, Chenwei, et al. "SegNet Network Architecture for Deep Learning Image Segmentation and Its Integrated Applications and Prospects." Academic Journal of Science and Technology 9.2 (2024): 224-229.

[24] Wang, Yong, et al. "Autonomous Driving System Driven by Artificial Intelligence Perception Fusion." Academic Journal of Science and Technology 9.2 (2024): 193-198.

[25] Duan, Shiheng, et al. "THE INNOVATIVE MODEL OF ARTIFICIAL INTELLIGENCE COMPUTER EDUCATION UNDER THE BACKGROUND OF EDUCATIONAL INNOVATION." 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.. 2024.

[26] Zhang, Quan, et al. "Application of the AlphaFold2 Protein Prediction Algorithm Based on Artificial Intelligence." Journal of Theory and Practice of Engineering Science 4.02 (2024): 58-65.

[27] Bao, Qiaozhi, et al. "Exploring ICU Mortality Risk Prediction and Interpretability Analysis Using Machine Learning." (2024).

[28] Zhou, Y., Osman, A., Willms, M., Kunz, A., Philipp, S., Blatt, J., & Eul, S. (2023). Semantic Wireframe Detection.

[29] Zhang, Y., Gono, R., & Jasiński, M. (2023). An Improvement in Dynamic Behavior of Single Phase PM Brushless DC Motor Using Deep Neural Network and Mixture of Experts. IEEE Access.

[30] Zhu, Mengran, et al. "THE APPLICATION OF DEEP LEARNING IN FINANCIAL PAYMENT SECURITY AND THE CHALLENGE OF GENERATING ADVERSARIAL NETWORK MODELS." The 8th International scientific and practical conference “Priority areas of research in the scientific activity of teachers”(February 27–March 01, 2024) Zagreb, Croatia. International Science Group. 2024. 298 p.. 2024.

[31] K. Xu, X. Wang, Z. Hu and Z. Zhang, "3D Face Recognition Based on Twin Neural Network Combining Deep Map and Texture," 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 2019, pp. 1665-1668, doi: 10.1109/ICCT46805.2019.8947113.