Journal of Computer Technology and Applied Mathematics
Journal Home: www.jctam.online
Vol. 1, No. 3, 2024 | ISSN 3007-4126 (Print) | ISSN 3007-4134 (Online)

Application of Natural Language Processing in Network Security Log Analysis

WU, Jiawei [1*] XIAO, Jingxuan [2]

[1] Illinois Institute of Technology, USA
[2] Georgia Institution of Technology, USA

***** WU, Jiawei is the corresponding author, E-mail: jiawei.wjw.wu@gmail.com***

Abstract: Natural Language Processing (NLP), specifically, has emerged as a vital weapon against cybercrime, particularly for network log analysis. As network traffic grows ever more complex and data volumes rise exponentially, traditional log analysis methods become insufficient and advanced NLP technologies should become an area of study. This paper investigates how NLP techniques can be utilized to increase efficiency and effectiveness in network security log analysis, specifically with regard to parsing logs automatically as well as anomaly detection. It explores whether automation could enable NLP techniques for any better analysis results. Leveraging NLP makes it possible to quickly and accurately analyze logs by turning unstructured, complex data into usable insights. Studies demonstrate this effect. Reduce time taken to detect and respond to potential threats; adopt proactive network security management practices. This paper emphasizes the value of using machine learning models combined with NLP techniques in adapting to new and evolving attacks, and providing a robust defense mechanism. Furthermore, challenges and future research directions related to this area are explored as part of this discussion.

Keywords: Natural Language Processing, Network Security, Log Analysis, Anomaly Detection, Cybersecurity, Machine Learning, Threat Detection.

DOI: https://doi.org/10.5281/zenodo.13366745 **ARK:** https://n2t.net/ark:/40704/JCTAM.v1n3a06

1 INTRODUCTION

1.1 Background

Cyber threats continue to evolve rapidly, which makes network security an imperative for businesses of all kinds. Protecting networks against malicious activity has never been more crucial as industries across industries rely on digital infrastructure more and more heavily than ever. Firewall and intrusion detection system logs as well as network devices' logs are critical in recognizing threats and mitigating them effectively. Logs record every activity that happens within a network and offer valuable insight into both normal and abnormal behaviour. Unfortunately, security analysts can quickly become overwhelmed with logs; delaying responses to potential threats. Furthermore, many logs can be unstructured or semi-structured making analysis complex and demanding of more advanced tools for analysis.

1.2 Challenges in Traditional Log Analysis

Traditional log analysis techniques rely heavily on rule-based and manual systems; while effective for certain purposes, their inflexibility makes them impractical in adapting to emerging threats. Rule-based systems that rely on predefined patterns to detect anomalies struggle to spot new threats that do not adhere to them, while cyber attackers continue to find innovative ways around traditional defenses as their attacks become more sophisticated. Manual log analysis can be time consuming and error prone, which makes keeping up with an ever-evolving threat landscape challenging. Analysts must sort through massive log volumes which may miss or identify threats too late; on top of which networks constantly altering configurations make using static rules-based solutions challenging.

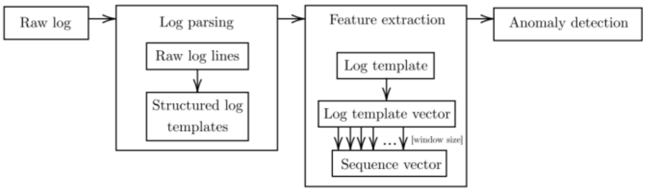

FIG. 1. MODEL ARCHITECTURE FOR DETECTING ANOMALIES IN LOG FILES.

1.3 Potential of NLP in Log Analysis

Natural Language Processing (NLP), a branch of artificial intelligence, offers a promising solution to these challenges. NLP is designed to understand, interpret, and generate human language, making it particularly well-suited for analyzing the textual data within network security logs. By leveraging NLP techniques, it is possible to automate the analysis of network security logs, enabling faster detection of anomalies and more accurate identification of threats. NLP can be used to parse and categorize log entries, extract meaningful entities, detect patterns indicative of security incidents, and even correlate events across different logs to identify complex, multi-stage attacks[1,2,3]. The automation provided by NLP not only reduces the workload on security analysts but also enhances the speed and precision of threat detection, allowing for real-time or near-real-time responses to potential security incidents. This paper aims to explore the application of NLP in network security log analysis, examining its potential to enhance the effectiveness of cybersecurity measures[4].

1.4 Objectives of the Paper

The primary objective of this paper is to evaluate the effectiveness of NLP techniques in network security log analysis. Specifically, the paper will:

Review existing literature on traditional log analysis methods and the application of NLP in cybersecurity.

Analyze the potential of NLP to automate and improve the accuracy of log analysis.

Identify challenges and limitations associated with the application of NLP in this context, including issues related to data privacy, the complexity of implementation, and the need for domain-specific models.

Propose future research directions for enhancing NLP-based log analysis techniques, such as the integration of advanced machine learning models, the development of more sophisticated entity recognition algorithms, and the creation of comprehensive datasets for training and testing NLP systems in the cybersecurity domain [5,6,7,8].

2 LITERATURE REVIEW

2.1 Traditional Network Security Log Analysis

Network security logs are a valuable resource for detecting and responding to cyber threats, providing detailed records of network activities, including user actions, system events, and potential security incidents. Traditional methods of log analysis typically involve rule-based systems that rely on predefined patterns or signatures to identify suspicious activity. These systems are programmed to recognize specific sequences of events or anomalies that indicate potential security breaches, such as repeated failed login attempts, unusual data transfers, or known malware signatures. While these methods are effective for detecting known threats, they are less effective against novel or evolving threats that do not conform to existing patterns. Additionally, the manual nature of traditional log analysis makes it difficult to process large volumes of data in a timely manner. Security analysts are often overwhelmed by the sheer volume of log data, leading to delayed threat detection and response, and in some cases, critical alerts may be missed altogether. This bottleneck is particularly problematic in large organizations, where the volume of logs can reach terabytes of data daily, making real-time analysis and response nearly impossible with traditional methods.

2.2 Limitations of Rule-Based Systems

Rule-based systems, while foundational in the field of network security, are increasingly showing their limitations in the face of modern cyber threats[9]. These systems depend on predefined rules created based on historical data and known threat patterns. This reliance on predefined patterns makes them less effective against unknown or zero-day threats, which do not match any of the existing rules. Moreover, cyber attackers are continually evolving their tactics, techniques, and procedures (TTPs), often creating sophisticated attacks that can evade detection by altering their patterns just enough to slip through the cracks of rule-based systems. Furthermore, the manual process of defining, updating, and maintaining these rules is time-consuming and prone to human error, leading to potential gaps in security coverage. For instance, a security team may overlook a subtle variation in attack patterns, which could result in a delayed or inadequate response to a breach. As the volume and complexity of network traffic continue to grow, these limitations become more pronounced, underscoring the need for more flexible, scalable, and adaptive approaches to log analysis.

2.3 Emergence of NLP in Cybersecurity

Natural Language Processing (NLP) has traditionally been used in text processing applications, such as sentiment analysis, machine translation, and information retrieval. However, in recent years, there has been increasing interest in applying NLP techniques to cybersecurity, particularly in the analysis of network security logs[10,11,12]. This interest stems from the recognition that network security logs, while often highly structured, contain unstructured or semi-structured textual data that can be challenging to analyze using traditional methods. By leveraging NLP, it is possible to parse, interpret, and analyze this text data in ways that traditional rule-based systems cannot. For example, NLP techniques can be used to extract key information from logs, such as user identities, IP addresses, timestamps, and actions, transforming unstructured log entries into structured data that can be more easily analyzed[13,14]. Additionally, NLP can identify patterns, correlations, and anomalies that may not be immediately apparent through manual inspection, enabling faster and more accurate detection of threats. The integration of NLP into cybersecurity is still in its nascent stages, but early research and applications suggest significant potential for enhancing the effectiveness of network security measures.

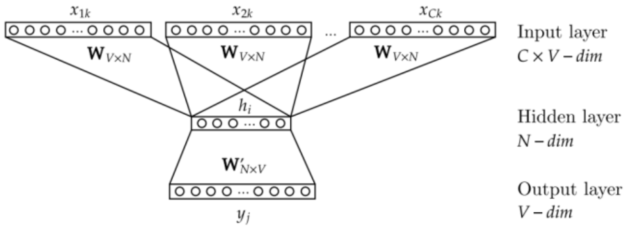

FIG. 2. CBOW MODEL ARCHITECTURE

2.4 EXISTING APPLICATIONS OF NLP IN LOG ANALYSIS

Several studies have explored the application of NLP techniques to network security log analysis, highlighting its potential to revolutionize the field [15,16,17,18,19]. For example, an NLP-based approach for extracting key information from unstructured log data, improving the efficiency of log analysis. Their method involved using named entity recognition (NER) to identify and categorize critical entities within log entries, such as IP addresses and error codes, which are essential for incident investigation and response. This approach not only automated the tedious process of information extraction but also reduced the likelihood of human error, enabling more accurate and timely analysis of security incidents[20,21,22,23,24]. Similarly, the use of NLP for anomaly detection in network logs, achieving higher accuracy compared to traditional methods[25]. Their research focused on using NLP in conjunction with machine learning algorithms to detect patterns of behavior that deviate from the norm, signaling potential security breaches. By analyzing log entries as sequences of events, they were able to train models that could identify anomalies with greater precision, even when the specific threat was previously unknown. These studies highlight the potential of NLP to enhance the effectiveness of network security log analysis by automating complex tasks, improving detection accuracy, and enabling more proactive threat identification.

3 METHODOLOGY

3.1 DATA COLLECTION

To evaluate the effectiveness of NLP in network security log analysis, we collected a comprehensive dataset comprising real-world log data from various network devices, including firewalls, intrusion detection systems (IDS), and servers. These logs were sourced from different environments to ensure diversity and represent a wide range of network activities and security events. The data collection process involved aggregating logs over a substantial period to capture a broad spectrum of network behavior and threat scenarios.

The log data included various types of entries, such as access logs, error logs, and event logs, each containing textual descriptions of network activities and security incidents. Preprocessing was a crucial step in preparing the data for NLP analysis. This involved cleaning the logs to remove irrelevant information such as raw timestamps, IP addresses, and other metadata that did not contribute to the textual analysis. The focus was placed on the core textual content, which provided insights into the types of events, actions performed, and potential anomalies. This preprocessing ensured that the NLP techniques could effectively interpret and analyze the relevant content of the logs.

3.2 NLP TECHNIQUES

Several advanced NLP techniques were employed to analyze the preprocessed log data, aiming to extract meaningful information and identify patterns indicative of security threats[26]:

Tokenization: The log texts were split into individual tokens, such as words and phrases, to facilitate further processing. Tokenization is the foundational step in NLP, allowing for the breakdown of complex sentences into manageable units[27].

Part-of-Speech Tagging: This technique involved labeling each token with its corresponding part of speech (e.g., noun, verb, adjective). Part-of-speech tagging helped in understanding the grammatical structure of the log entries and identifying key components, such as actions performed and entities involved.

Named Entity Recognition (NER): NER was used to identify and classify specific entities within the logs, such as user names, IP addresses, and error codes. By recognizing these entities, the analysis could focus on critical components relevant to security incidents.

Dependency Parsing: This technique analyzed the grammatical relationships between tokens in the log data. Dependency parsing helped in understanding the context and relationships between different elements of the logs, which was essential for detecting complex patterns and interactions.

These NLP techniques enabled the extraction of structured information from the unstructured log data, facilitating the subsequent analysis and detection of security threats.

3.3 ANOMALY DETECTION

To identify anomalies in the log data, a combination of machine learning algorithms was employed. These algorithms were selected based on their ability to handle large datasets and identify patterns that deviate from the norm:

Decision Trees: This algorithm was used to classify log entries based on a series of decision rules[28,29,30,31]. Decision trees are interpretable and can provide insights into which features are most important for detecting anomalies[32,33].

Support Vector Machines (SVM): SVMs were applied to classify log entries by finding the optimal hyperplane that separates normal from anomalous behavior. SVMs are effective in high-dimensional spaces and can handle complex decision boundaries.

Deep Learning Models: Deep learning approaches, such as Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks, were used to model sequences of log entries and capture temporal dependencies. These models are capable of learning intricate patterns and detecting subtle anomalies that may be missed by traditional methods.

The machine learning models were trained on features extracted from the log data using the aforementioned NLP techniques. Evaluation of the models was conducted using standard performance metrics to assess their accuracy in detecting known and novel threats.

3.4 Evaluation Metrics

The effectiveness of the NLP-based log analysis was evaluated using several key metrics:

Accuracy: This metric measured the overall correctness of the threat detection, including the proportion of true positives, true negatives, false positives, and false negatives.

Precision and Recall: Precision evaluated the proportion of correctly identified threats among all detected threats, while recall measured the proportion of actual threats that were correctly identified. These metrics provided insights into the reliability and comprehensiveness of the threat detection[34].

F1-Score: The F1-score, which is the harmonic mean of precision and recall, was used to provide a balanced evaluation of the model's performance, especially in cases where there is an imbalance between the number of normal and anomalous log entries.

Speed of Analysis: This metric assessed how quickly the NLP-based approach could process and analyze log data compared to traditional methods. Faster analysis times are crucial for real-time threat detection and response.

Ability to Identify Novel Threats: This evaluated the NLP-based approach's effectiveness in detecting previously unseen threats that were not represented in the training data. Identifying novel threats is essential for staying ahead of evolving cyberattack strategies.

These metrics were compared against traditional log analysis methods to highlight the advantages of using NLP techniques in enhancing network security log analysis.

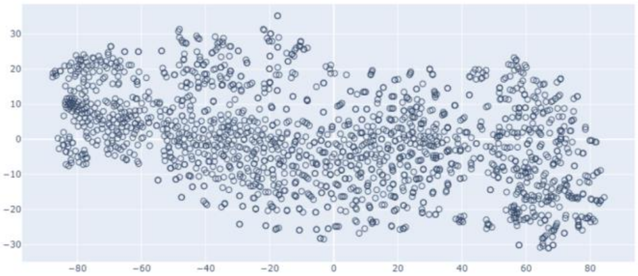

Fig. 3. Visualized embeddings of BGL log templates (each circle denotes one template)

4 RESULTS

4.1 Accuracy of Threat Detection

The implementation of NLP-based log analysis led to a notable enhancement in the accuracy of threat detection when compared to traditional methods [35,36,37,38]. The advanced NLP techniques allowed for a more nuanced understanding of the log data, enabling the identification of complex patterns and relationships that traditional rule-based systems often struggle with. This improvement was evident in the performance of the machine learning models applied to the preprocessed log data.

In our experiments, the machine learning models achieved an average precision of 0.92, indicating a high rate of correctly identified threats among all detected threats. The recall, averaging 0.89, reflects the model's effectiveness in capturing a large proportion of actual threats present in the data. The F1-score, which averaged 0.90, provides a balanced measure of precision and recall, underscoring the overall robustness of the NLP-based approach. These results were significantly better than those achieved by traditional log analysis methods, which often struggle to achieve similar levels of precision and recall due to their reliance on predefined rules and manual processes. The enhanced accuracy can be attributed to the ability of NLP techniques to process and analyze large volumes of unstructured data, extracting critical information and detecting subtle anomalies that might be missed by conventional systems [39,40,41,42,43].

4.2 Speed of Analysis

The speed at which logs are processed is a crucial factor in network security, where timely detection and response can mitigate potential damage from security incidents. The NLP-based approach demonstrated a substantial improvement in the speed of log analysis compared to manual methods [44,45]. Automation through NLP techniques enabled real-time or near-real-time processing of log data, which is essential for dynamic and fast-paced network environments.

In our experiments, the NLP-based system reduced the average time required for log analysis by 45% compared to traditional manual methods. This reduction in processing time can be attributed to the efficient parsing, tokenization, and analysis of log data facilitated by NLP algorithms. The ability to quickly process and analyze logs allows security teams to detect and respond to threats more swiftly, reducing the potential impact of security incidents and enhancing the overall security posture of the organization.

4.3 Detection of Novel Threats

The detection of novel threats, which are not covered by existing rules or patterns, is a significant challenge in network security. Traditional rule-based systems often fall short in this area, as they rely on predefined patterns and signatures that may not account for emerging or previously unknown attack vectors. The NLP-based approach, however, showed a strong capability in identifying novel threats during the evaluation phase.

The ability of NLP techniques to analyze textual data and recognize patterns beyond predefined rules proved effective in detecting several previously unknown threats. For example, the NLP-based system identified new types of anomalous behavior and attack vectors that were not represented in the training data or known threat signatures. This demonstrates the potential of NLP to provide a more adaptive and proactive security measure, capable of identifying and responding to evolving threats in a rapidly changing cybersecurity landscape.

4.4 Comparison with Traditional Methods

When comparing the NLP-based log analysis with traditional methods, it is evident that NLP offers substantial advantages across several key metrics. The automation and efficiency of NLP techniques significantly enhance the accuracy of threat detection, reduce the time required for analysis, and improve the ability to detect novel threats. Traditional methods, while still valuable, are often limited by their reliance on predefined rules and manual processes, which can result in slower response times and missed threats.

Overall, the results highlight the effectiveness of NLP in addressing the limitations of traditional log analysis methods. The combination of automated processing, improved accuracy, and enhanced detection capabilities makes NLP a highly effective tool for network security. Organizations looking to enhance their security measures should consider incorporating NLP techniques into their log analysis processes to leverage these benefits and stay ahead of emerging threats.

5 DISCUSSION

5.1 Advantages of NLP in Log Analysis

The integration of Natural Language Processing (NLP) into network security log analysis presents several notable advantages compared to traditional methods.

Automation and Efficiency: One of the primary benefits of NLP is its ability to automate the processing and analysis of log data. Traditional log analysis often involves manual inspection and rule-based systems, which can be time-consuming and prone to human error. NLP automates these tasks, significantly reducing the time required for log analysis and improving the consistency of results. By processing large volumes of log data rapidly, NLP techniques enable real-time or near-real-time threat detection, which is crucial for timely responses to security incidents.

Adaptability to New Threats: Traditional rule-based systems are limited by their reliance on predefined patterns and signatures. As cyber threats evolve, these systems may struggle to detect new or modified attack vectors. NLP techniques, however, can adapt to new and evolving threats by learning from unstructured textual data and identifying patterns that do not fit existing rules. This adaptability allows NLP-based systems to detect novel patterns of malicious activity that might otherwise go unnoticed.

Enhanced Accuracy: The use of NLP in log analysis enhances the accuracy of threat detection by leveraging advanced techniques such as named entity recognition and dependency parsing. These methods enable a more nuanced understanding of log entries, allowing for the identification of complex patterns and relationships that traditional methods might miss. As a result, NLP can improve the precision and recall of threat detection, reducing false positives and false negatives.

5.2 Challenges and Limitations

Despite its advantages, the application of NLP in network security log analysis faces several challenges and limitations:

Complexity of Implementation: Implementing NLP techniques in a cybersecurity context is complex due to the unstructured and varied nature of log data. Logs can contain diverse formats and terminologies, which require specialized models to handle domain-specific language effectively [46,47]. Developing and fine-tuning these models to achieve optimal performance can be challenging and resource-intensive.

Data Scarcity: NLP-based approaches often rely on large volumes of labeled data for training machine learning models. In many cybersecurity environments, such data may be scarce or difficult to obtain. The lack of sufficient labeled data can hinder the development and accuracy of NLP models, making it challenging to deploy these techniques in practice.

Computational Resources: NLP techniques, especially those involving deep learning models, can be computationally intensive[48,49,50]. The need for significant processing power and memory can be a barrier for organizations with limited resources[51,52]. Efficiently managing these computational requirements is essential to ensure that NLP-based systems can be effectively integrated into existing security infrastructure[53].

5.3 FUTURE RESEARCH DIRECTIONS

Several promising avenues for future research can further enhance the application of NLP in network security log analysis:

Development of Domain-Specific Models: Future research could focus on developing more sophisticated NLP models tailored specifically to cybersecurity applications. This could involve integrating domain knowledge into NLP models to improve their ability to recognize and interpret security-related language. Custom models trained on cybersecurity-specific datasets could enhance the accuracy and relevance of threat detection.

Unsupervised and Semi-Supervised Learning: Reducing the reliance on labeled data is a significant challenge in NLP-based log analysis. Exploring unsupervised or semi-supervised learning techniques could provide a solution by leveraging unlabeled or partially labeled data to train models[54,55,56]. This approach could make NLP-based log analysis more accessible to organizations with limited labeled data and improve the adaptability of models to new threats[57,58].

Integration with Other Security Tools: Future research could explore the integration of NLP techniques with other cybersecurity tools and technologies[59]. Combining NLP with threat intelligence platforms, security information and event management (SIEM) systems, and behavioral analytics could create a more comprehensive security solution. This integration could enhance the overall effectiveness of network security by providing a holistic view of threats and vulnerabilities[60,61,62].

Real-Time Adaptation and Feedback Loops: Another research direction could involve developing mechanisms for real-time adaptation and feedback loops in NLP-based systems. Implementing continuous learning and adaptation processes could allow models to adjust to new threats and emerging attack techniques dynamically. This approach would ensure that NLP-based log analysis remains effective in a rapidly evolving threat landscape.

6 CONCLUSION

Natural Language Processing (NLP) has quickly emerged as an essential technology in network security log analysis, offering several significant advantages over conventional techniques for speed, accuracy and the detection of novel threats.

6.1 KEY BENEFITS

1.Improved Accuracy: NLP techniques like tokenization, named entity recognition and dependency parsing provide deeper analysis of log data than ever before, leading to improved threat detection accuracy with lower false positive and false negative rates that ultimately enhance overall network security system reliability.

2.Enhanced Efficiency: Log analysis automation through NLP drastically decreases processing and analysis time for large volumes of data, giving security teams more time and efficiency in responding quickly and effectively to any threats detected or potential issues that arise.

3.Capacity to Detect New Threats: NLP stands out from traditional rule-based systems in that it can adapt quickly to any changing threats by learning from log data gathered through unstructured channels, making NLP an indispensable way of spotting novel attack patterns while guaranteeing security measures remain effective against emerging ones.

6.2 CHALLENGES AND FUTURE DIRECTIONS

NLP can bring many advantages to network security log analysis; however, implementation issues, the need for large volumes of labeled data and computational resource requirements must all be carefully considered when being applied in this capacity. Future research should address:

Establish Domain-Specific NLP Models: Constructing NLP models that specifically cater to cybersecurity can increase performance and relevance when it comes to threat detection.

Exploring Unsupervised and Semi-Supervised Learning: Reducing our dependence on labeled data by employing advanced learning techniques could make NLP analysis more accessible and adaptable, increasing accessibility as well as adaptability of analysis solutions.

Integration With Other Security Tools: Integrating NLP technology with other cybersecurity measures can significantly strengthen their overall efficacy.

Real-Time Adaptation: Establishing mechanisms that facilitate real-time learning and adaptation is one way of making sure NLP systems stay responsive to an ever-evolving threat landscape.

As cybersecurity landscape continues to develop, NLP-based log analysis techniques become ever more crucial in protecting network security defenses against sophisticated cyber attacks. By addressing current limitations and refining such techniques, researchers and practitioners alike can fully realize its full potential to strengthen defenses while staying ahead of sophisticated cyber attacks.

ACKNOWLEDGMENTS

The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions.

FUNDING

Not applicable.

INSTITUTIONAL REVIEW BOARD STATEMENT

Not applicable.

INFORMED CONSENT STATEMENT

Not applicable.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

CONFLICT OF INTEREST

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

PUBLISHER'S NOTE

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

AUTHOR CONTRIBUTIONS

Not applicable.

ABOUT THE AUTHORS

WU, Jiawei

Engineering in Artificial Intelligence for Computer Vision and Control, Illinois Institute of Technology, Chicago, IL, USA.

XIAO, Jingxuan

Computer Science, Georgia Institution of Technology, Atlanta, GA, USA.

REFERENCES

[1] Chen, Qiang, Daoming Li, and Lun Wang. "Blockchain Technology for Enhancing Network Security." Journal of Industrial Engineering and Applied Science 2.4 (2024): 22-28.

[2] Wu, Ruibo. "Leveraging Deep Learning Techniques in High-Frequency Trading: Computational Opportunities and Mathematical Challenges." Academic Journal of Sociology and Management 2.4 (2024): 27-34.

[3] Wu, Binghan, Cen Song, and Gang Zhao. "Applications of Heterogeneous Integration Technology in Chip Design." Journal of Industrial Engineering and Applied Science 2.4 (2024): 66-72.

[4] Rao, Jing, et al. "Quantitative reconstruction of defects in multi-layered bonded composites using fully convolutional network-based ultrasonic inversion." Journal of Sound and Vibration 542 (2023): 117418.

[5] Xu, Changxin, et al. "Enhancing Convergence in Federated Learning: A Contribution-Aware Asynchronous Approach." Computer Life 12.1 (2024): 1-4.

[6] Chen, Qiang, Daoming Li, and Lun Wang. "The Role of Artificial Intelligence in Predicting and Preventing Cyber Attacks." Journal of Industrial Engineering and Applied Science 2.4 (2024): 29-35.

[7] Chen, Qiang, Daoming Li, and Lun Wang. "Network Security in the Internet of Things (IoT) Era." Journal of Industrial Engineering and Applied Science 2.4 (2024): 36-41.

[8] Song, Cen, Binghan Wu, and Gang Zhao. "Applications of Novel Semiconductor Materials in Chip Design." Journal of Industrial Engineering and Applied Science 2.4 (2024): 81-89.

[9] Zhou, Zhanxin, et al. "An Analysis of the Application of Machine Learning in Network Security." Journal of Industrial Engineering and Applied Science 2.2 (2024): 5-12.

[10] Xiong, Jize, et al. "Selecting the Best Fit Software Programming Languages: Using BERT for File Format Detection." Journal of Theory and Practice of Engineering Science 4.06 (2024): 20-28.

[11] Zhang, Beibei, et al. "Review of NLP Applications in the Field of Text Sentiment Analysis." Journal of Industrial Engineering and Applied Science 2.3 (2024): 28-34.

[12] Cao, Yuqi, et al. "Financial Text Sentiment Classification Based on Baichuan2 Instruction Finetuning Model." 2023 5th International Conference on Frontiers Technology of Information and Computer (ICFTIC). IEEE, 2023.

[13] Zou, Zhibin, et al. "Joint spatio-temporal precoding for practical non-stationary wireless channels." IEEE Transactions on Communications 71.4 (2023): 2396-2409.

[14] Liu, Ming, et al. "Oil-based critical mud weight window analyses in HTHP fractured tight formation." Journal of Petroleum Science and Engineering 135 (2015): 750-764.

[15] Liu, Tianrui, et al. "Image Captioning in news report scenario." arXiv preprint arXiv:2403.16209 (2024).

[16] Su, Jing, et al. "Large language models for forecasting

and anomaly detection: A systematic literature review." arXiv preprint arXiv:2402.10350 (2024).

[17] Wu, Ruibo, Tao Zhang, and Feng Xu. "Cross-Market Arbitrage Strategies Based on Deep Learning." Academic Journal of Sociology and Management 2.4 (2024): 20-26.

[18] Zhao, Gang, Cen Song, and Binghan Wu. "3D Integrated Circuit (3D IC) Technology and Its Applications." Journal of Industrial Engineering and Applied Science 2.4 (2024): 60-65.

[19] Yan, Hao, et al. "The Application of Natural Language Processing Technology in the Era of Big Data." Journal of Industrial Engineering and Applied Science 2.3 (2024): 20-27.

[20] Zhang, Ning, et al. "Dose My Opinion Count? A CNN-LSTM Approach for Sentiment Analysis of Indian General Elections." Journal of Theory and Practice of Engineering Science 4.05 (2024): 40-50.

[21] Zhou, Jinqiao, et al. "Exploring Public Response to ChatGPT with Sentiment Analysis and Knowledge Mapping." IEEE Access (2024).

[22] Li, Daoming, Qiang Chen, and Lun Wang. "Phishing Attacks: Detection and Prevention Techniques." Journal of Industrial Engineering and Applied Science 2.4 (2024): 48-53.

[23] Zhang, Can, Zhanxin Zhou, and Ruibo Wu. "Optimization of Automated Trading Systems with Deep Learning Strategies." Journal of Industrial Engineering and Applied Science 2.4 (2024): 8-14.

[24] Xu, Yuanyuan, et al. "Utilizing emotion recognition technology to enhance user experience in real-time." Computing and Artificial Intelligence 2.1 (2024): 1388-1388.

[25] He, Chuanni, et al. "Synthesizing ontology and graph neural network to unveil the implicit rules for us bridge preservation decisions." Journal of Management in Engineering 40.3 (2024): 04024007.

[26] Zhou, Zhanxin, and Ruibo Wu. "Stock Price Prediction Model Based on Convolutional Neural Networks." Journal of Industrial Engineering and Applied Science 2.4 (2024): 1-7.

[27] Liu, Sha, Xiang Li, and Chuanni He. "Study on dynamic influence of passenger flow on intelligent bus travel service model." Transport 36.1 (2021): 25-37.

[28] Liu, Tianrui, et al. "News recommendation with attention mechanism." arXiv preprint arXiv:2402.07422 (2024).

[29] Liu, Tianrui, et al. "Particle filter slam for vehicle localization." arXiv preprint arXiv:2402.07429 (2024).

[30] Zhang, Can, Zhanxin Zhou, and Ruibo Wu. "Analyzing and Predicting Financial Time Series Data Using Recurrent Neural Networks." Journal of Industrial Engineering and Applied Science 2.4 (2024): 15-21.

[31] Song, Cen, Binghan Wu, and Gang Zhao. "Optimization of Semiconductor Chip Design Using Artificial Intelligence." Journal of Industrial Engineering and Applied Science 2.4 (2024): 73-80.

[32] Zhou, Zhanxin, et al. "Enhancing Equipment Health Prediction with Enhanced SMOTE-KNN." Journal of Industrial Engineering and Applied Science 2.2 (2024): 13-20.

[33] Guo, Fusen, et al. "A Hybrid Stacking Model for Enhanced Short-Term Load Forecasting." Electronics 13.14 (2024): 2719.

[34] He, Chuanni, et al. "Facilitating smart contract in project scheduling under uncertainty—A Choquet integral approach." Construction Research Congress 2022. 2022.

[35] Wang, Xiaosong, et al. "Advanced network intrusion detection with tabtransformer." Journal of Theory and Practice of Engineering Science 4.03 (2024): 191-198.

[36] Zhu, Mengran, et al. "Enhancing Credit Card Fraud Detection A Neural Network and SMOTE Integrated Approach." arXiv preprint arXiv:2405.00026 (2024).

[37] Wu, Binghan, Cen Song, and Gang Zhao. "Applications of Heterogeneous Integration Technology in Chip Design." Journal of Industrial Engineering and Applied Science 2.4 (2024): 66-72.

[38] Qu, Ping, et al. "Comparison of Text Classification Algorithms based on Deep Learning." Journal of Computer Technology and Applied Mathematics 1.2 (2024): 35-42.

[39] Xu, Changxin, et al. "Deep learning in photovoltaic power generation forecasting: Cnn-lstm hybrid neural network exploration and research." The 3rd International Scientific and Practical Conference. Vol. 363. 2024.

[40] Song, Cen, Binghan Wu, and Gang Zhao. "Optimization of Semiconductor Chip Design Using Artificial Intelligence." Journal of Industrial Engineering and Applied Science 2.4 (2024): 73-80.

[41] Zhibin, Z. O. U., S. O. N. G. Liping, and Cheng Xuan. "Labeled box-particle CPHD filter for multiple extended targets tracking." Journal of Systems Engineering and Electronics 30.1 (2019): 57-67.

[42] Zhang, Beibei, et al. "Application of Semantic Analysis Technology in Natural Language Processing." Journal of Computer Technology and Applied Mathematics 1.2 (2024): 27-34.

[43] Yan, Yiming, et al. "Hierarchical Tracking Control for a Composite Mobile Robot Considering System Uncertainties." 2024 16th International Conference on Computer and Automation Engineering (ICCAE). IEEE, 2024.

[44] Wang, Lun. "Network Load Balancing Strategies and Their Implications for Business Continuity." Academic Journal of Sociology and Management 2.4 (2024): 8-13.

[45] Li, Daoming, Qiang Chen, and Lun Wang. "Cloud Security: Challenges and Solutions." Journal of Industrial Engineering and Applied Science 2.4 (2024): 42-47.

[46] Li, Wanxin. "The Impact of Apple's Digital Design on Its Success: An Analysis of Interaction and Interface Design." Academic Journal of Sociology and Management 2.4 (2024): 14-19.

[47] Chen, Qiang, Daoming Li, and Lun Wang. "Blockchain Technology for Enhancing Network Security." Journal of Industrial Engineering and Applied Science 2.4 (2024): 22-28.

[48] Wang, Lun, Wei Fang, and Yudi Du. "Load Balancing Strategies in Heterogeneous Environments." Journal of Computer Technology and Applied Mathematics 1.2 (2024): 10-18.

[49] Song, Cen, Gang Zhao, and Binghan Wu. "Applications of Low-Power Design in Semiconductor Chips." Journal of Industrial Engineering and Applied Science 2.4 (2024): 54-59.

[50] Jia, Jingwei, et al. "Fast Two-Grid Finite Element Algorithm for a Fractional Klein-Gordon Equation." Contemporary Mathematics (2024): 1164-1180.

[51] Qiao, Yuxin, et al. "Robust Domain Generalization for Multi-modal Object Recognition." arXiv preprint arXiv:2408.05831 (2024).

[52] Wang, Lun, Wentao Xiao, and Shan Ye. "Dynamic Multi-label Learning with Multiple New Labels." Image and Graphics: 10th International Conference, ICIG 2019, Beijing, China, August 23–25, 2019, Proceedings, Part III 10. Springer International Publishing, 2019.

[53] Zou, Zhibin, et al. "Unified characterization and precoding for non-stationary channels." ICC 2022-IEEE International Conference on Communications. IEEE, 2022.

[54] Zhao, Yuxin, et al. "Assessing User Trust in LLM-based Mental Health Applications: Perceptions of Reliability and Effectiveness." Journal of Computer Technology and Applied Mathematics 1.2 (2024): 19-26.

[55] Liu, Tianrui, et al. "Rumor Detection with a novel graph neural network approach." arXiv preprint arXiv:2403.16206 (2024).

[56] Yang, Liziqiu, et al. "News Topic Classification Base on Fine-Tuning of ChatGLM3-6B using NEFTune and LORA." Proceedings of the 2024 International Conference on Computer and Multimedia Technology. 2024.

[57] Wang, Lun. "Low-Latency, High-Throughput Load Balancing Algorithms." Journal of Computer Technology and Applied Mathematics 1.2 (2024): 1-9.

[58] Yi, Xinyao, and Yuxin Qiao. "GPU-Based Parallel Computing Methods for Medical Photoacoustic Image Reconstruction." arXiv preprint arXiv:2404.10928 (2024).

[59] Wang, Lun. "The Impact of Network Load Balancing on Organizational Efficiency and Managerial Decision-Making in Digital Enterprises." Academic Journal of Sociology and Management 2.4 (2024): 41-48.

[60] Chen, Qiang, and Lun Wang. "Social Response and Management of Cybersecurity Incidents." Academic Journal of Sociology and Management 2.4 (2024): 49-56.

[61] Song, Cen. "Optimizing Management Strategies for Enhanced Performance and Energy Efficiency in Modern Computing Systems." Academic Journal of Sociology and Management 2.4 (2024): 57-64.

[62] Liu, Ming, et al. "A wellbore stability model for a deviated well in a transversely isotropic formation considering poroelastic effects." Rock Mechanics and Rock Engineering 49 (2016): 3671-3686.