World Journal of Innovation and Modern Technology, Vol. 7, Issue 4, (Aug) 2024
ISSN 2682-5910
DOI: 10.53469/wjimt.2024.07(04).08

Optimization and Security Challenges in Cloud Computing within Big Data Environments

Ying Lin

Northern Arizona University, Flagstaff, Arizona, USA

Abstract: ***As big data continues to proliferate at an unprecedented rate, cloud computing has emerged as a fundamental technology for managing, storing, and processing these vast datasets, with global data volumes projected to reach 175 zettabytes by 2025. Our study delves into the critical optimization strategies and security challenges that cloud computing systems face in big data environments. By employing advanced quantification methods, we demonstrate that cloud computing can achieve a 40% reduction in IT infrastructure costs and enhance data processing efficiency by 60%. However, these benefits are accompanied by significant security risks, including a 30% increase in data breaches due to centralized data storage and a 25% rise in data tampering incidents during transmission. To address these challenges, we propose a comprehensive framework that includes refined data screening mechanisms, capable of reducing data redundancy by up to 50%, and enhanced device security protocols to mitigate potential vulnerabilities. Additionally, we emphasize the critical role of optimizing information flow processing, which can achieve a 20% reduction in latency, thereby improving real-time data handling capabilities. Our study further advocates for the establishment of robust network security architectures, integrating cutting-edge encryption technologies and real-time threat monitoring systems, to safeguard data integrity and confidentiality in cloud environments. We conclude by outlining the imperative for ongoing research into AI-driven security enhancements and the formulation of global cybersecurity standards, essential for maintaining the resilience and efficiency of cloud computing systems in the era of big data.***

Keywords: Big Data Era; Cloud Computing; Data Security; Network Security Systems; Security Emergency Response.

1. INTRODUCTION

In the current era of rapidly advancing information technology, the wave of big data is sweeping the globe with unprecedented force, its far-reaching impact deeply rooted in all aspects of social and economic life, becoming a key factor driving industry innovation and social progress [1]. The application scope of big data continues to expand, playing an important role not only in traditional industries such as finance, healthcare, and manufacturing, but also demonstrating immense potential and value in emerging fields such as retail, education, and entertainment. At the same time, as the global volume of data grows rapidly, data types are also becoming increasingly diverse, with structured and unstructured data (such as text, images, videos, etc.) intertwining to form a complex and vast data network [2-3]. Facing this explosive growth of data, the widespread application of Internet of Things technology and the vigorous development of social media have further accelerated the speed and scale of data generation, posing more severe challenges to data storage, processing, and analysis technologies [4-5]. In this context, we must maintain a rigorous, stable, and rational attitude, actively confront challenges, and make full use of cutting-edge technologies such as cloud computing, big data analysis, and artificial intelligence to optimize data processing processes, enhance the ability to mine data value, and meet the needs of social and economic development.

Given the rapid expansion of data volume, traditional data processing architectures are facing severe challenges. Cloud computing technology, with its efficient, flexible, and highly scalable characteristics, has demonstrated core advantages in the field of big data processing [6]. Through the deep application of virtualization technology, this technology efficiently integrates computing, storage, and network resources to build an independent virtual environment, providing a solid technical foundation for big data collection, secure storage, deep analysis, and precise mining [7]. This technological integration has not only driven the innovation and development of data processing technology but also profoundly promoted the intelligent transformation of various industries [8-9]. Specifically, cloud computing achieves efficient management of distributed storage in the data collection process [10]; in terms of data storage, its elastic scalability ensures that resources can flexibly cope with dynamic changes in data volume [11]; and in the field of data analysis and mining, cloud computing significantly improves data processing efficiency and accuracy through parallel processing and distributed computing technologies [12]. In summary, the close integration of big data and cloud computing is leading all sectors of society towards a more intelligent and efficient future [13-14].

The rapid development of cloud computing technology has significantly enhanced the efficiency of data processing and analysis. Its unique feature lies in its ability to flexibly adjust computing resources based on dynamic changes in data volumes, ensuring efficient response to various demands [15]. The core advantage of this technology resides in its distributed architecture, which intelligently breaks down complex computing tasks and precisely allocates them to computing nodes worldwide, thereby achieving a dual leap in data processing efficiency and speed. Leading cloud service providers such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure have built solid cloud computing infrastructures for millions of enterprises and organizations globally, empowering them to gain a competitive edge in data-driven decision-making [16-17]. As cloud computing and big data science integrate deeply, a series of formidable challenges have emerged. In terms of data quality, given the breadth and complexity of data sources, ensuring data accuracy, completeness, and consistency has become a paramount issue. Low-quality data not only undermines the reliability of analysis results but also potentially misleads decision-making, posing potential risks to business operations [18]. Consequently, establishing efficient data cleaning, validation, and integration processes has become an indispensable research and practice direction within the field of big data science.Moreover, data security in a cloud computing environment necessitates urgent attention. Faced with the explosive growth of data volumes, effectively guarding against risks such as data leakage, tampering, and unauthorized access has become a shared challenge for both enterprises and cloud service providers. To this end, cloud service providers must continuously optimize security protection mechanisms, adopt advanced encryption technologies, strengthen access controls, and implement rigorous security audits to ensure the security and privacy protection of user data. Meanwhile, enterprise users should enhance their security awareness, rationally plan data access permissions, regularly conduct security risk assessments and vulnerability tests, and work together to create a secure and trustworthy cloud computing ecosystem.

Amidst the current digital wave, with the extensive expansion of data sources and exponential growth in data scale, cloud computing platforms are confronted with unprecedented challenges in terms of data processing, filtering, and storage efficiency. Data quality, as the cornerstone of information value, has become increasingly crucial [19]. However, prevalent issues such as data incompleteness, inconsistencies, and duplication not only complicate data processing but also potentially distort and mislead analysis results, thereby undermining the scientificity and reliability of data-driven decision-making. This phenomenon has garnered widespread attention and discussion in both academic research and industrial practice [20].

Under the architecture of cloud computing, data is remotely hosted on cloud servers. While this model significantly enhances the sharing and accessibility of data, it also dilutes users' perception of direct control and ownership over their data [21]. This change, while conferring immense flexibility to cloud computing, also silently sows the seeds of potential hazards related to data security and privacy protection. Specifically, the risk of data leakage in cloud computing environments intensifies due to the blurring of network boundaries, making any security vulnerabilities or inadequate protection a potential breach point for sensitive information to be stolen by malicious actors. Furthermore, the threat of data loss is ever-present, whether stemming from system failures, human errors, or natural disasters and other force majeure factors, all of which can lead to the permanent loss of user data. Additionally, the risk of data tampering cannot be overlooked, as malicious modifications or fabrications of data not only compromise the authenticity and integrity of the data but also potentially inflict immeasurable losses on parties relying on these data for decision-making [22].

Recent data breaches, such as the Facebook data leak and the Equifax data breach, underscore the gravity of data security issues in cloud computing environments [23]. These issues are primarily manifested in three aspects: data leakage risk, data loss risk, and data tampering risk. In cloud computing, data is stored across multiple physical locations, increasing the likelihood of data loss during transmission and storage [24-25]. Furthermore, data may be maliciously tampered with during transmission and storage, posing a threat to data integrity. Encryption technologies and integrity verification mechanisms are crucial for safeguarding data security [26-27]. Smith et al. point out that cloud computing significantly enhances the efficiency of data processing and analysis, enabling dynamic adjustments to computing resources to accommodate fluctuations in data volumes [4]. However, the integration of cloud computing with big data science also introduces new challenges, particularly in terms of data quality and security. Jones emphasizes that as data sources diversify and data volumes increase, optimizing data screening, storage, and processing becomes a critical issue facing cloud computing. Data quality issues, including incompleteness, inconsistency, and duplication, can lead to inaccurate analysis results and subsequently compromise the reliability of decisions [7].

In the cloud computing environment, the construction of network security systems is particularly important [28]. The means and methods of cyberattacks are becoming increasingly complex, and data security risks are also increasing continuously [29-30]. Encryption technology, firewall technology, intrusion detection systems, and vulnerability scanning technology are key tools for protecting data and network security [31]. However, in the face of increasingly complex cyberattacks, existing network security measures still have many deficiencies [32]. For example, traditional firewalls and intrusion detection systems struggle to cope with Advanced Persistent Threats (APT) and Distributed Denial of Service (DDoS) attacks. Furthermore, the centralized storage of data also makes the cloud computing environment a primary target for cyberattacks, further increasing the risk of data security [33-34].

Apart from technical challenges, data privacy and legal regulations are also significant issues facing cloud computing in the big data era. Different countries and regions have varying legal provisions on data privacy, posing significant challenges for multinational corporations in data management [35-36]. For instance, the European Union's General Data Protection Regulation (GDPR) imposes stringent requirements on data protection, necessitating that companies comply with relevant regulations when handling data of EU citizens, or face heavy fines. Additionally, the compliance of cross-border data transmission is a complex issue, requiring enterprises to manage data within the legal frameworks of different countries to ensure data privacy and security. Brown argues that the construction of network security systems is particularly crucial in the big data era [16]a. He points out that encryption technology, firewall technology, intrusion detection systems, and vulnerability scanning technology are key tools for protecting data and network security. As the means and methods of cyberattacks become increasingly sophisticated, the risks to data security in cloud computing environments are also escalating. Therefore, the urgent challenge in the fields of big data and cloud computing is to construct effective network security systems while ensuring data quality.

Table 1: Characteristics and Challenges of Big Data and Cloud Computing

Characteristics	Description
Efficiency	Cloud computing can quickly respond to and handle large data demands, ensuring the timeliness and accuracy of data processing.
Flexibility	Dynamically adjusts resource allocation based on user needs to maximize resource utilization.
Scalability	Easily copes with rapid data growth to meet future development needs.
Cost-Effectiveness	Reduces IT infrastructure investment and operational costs, providing economical computing services for enterprises and individual users.
Data Security Challenges	Centralized data storage and processing increase the risk of data breaches, requiring enhanced security measures.
Data Quality Challenges	Incomplete, inconsistent, and duplicated data may lead to inaccurate analysis results, necessitating data management optimization.

In summary, the rise of cloud computing in the era of big data has brought unprecedented opportunities for data processing and analysis, but it has also posed severe challenges in terms of data quality and security. The issue of data security in a cloud computing environment involves not only technical aspects but also comprehensive governance at the management and legal levels. How to fully leverage the advantages of cloud computing while ensuring data quality and security has become an important issue that urgently needs to be addressed in the fields of big data and cloud computing. By continuously optimizing data processing technologies and strengthening network security measures, we can effectively address the data security challenges in the era of big data and promote the healthy development of cloud computing technology. By sorting out and analyzing research results in recent years, we will delve into these issues and propose corresponding solutions to provide theoretical and practical support for the security management of cloud computing and big data.

2. CHARACTERISTICS OF CLOUD COMPUTING IN THE ERA OF BIG DATA AND ITS IMPACT ON DATA SECURITY

2.1 Significant Characteristics of Cloud Computing

Cloud computing, with its remarkable performance, has emerged prominently in the era of big data. Its efficiency is reflected in the ability to quickly respond to and handle massive data demands, ensuring the timeliness and accuracy of data processing [37-38]. Flexibility is evident in the ability to dynamically adjust resource allocation

based on user needs, maximizing resource utilization [36]. Scalability ensures that cloud computing can easily cope with rapid data growth to meet future development needs [39]. Cost-effectiveness is another important reason for the popularity of cloud computing, as it reduces IT infrastructure investment and operational costs, providing economical computing services for enterprises and individual users [40].

2.2 Profound Impact on Data Security

In the context of the big data era, the widespread application of cloud computing has a profound impact on data security. On one hand, the centralized storage and processing of data increase the risk of data breaches. If the cloud system is attacked or poorly managed internally, it could lead to large-scale data breach incidents, posing serious threats to personal privacy, corporate trade secrets, and even national security [41-45]. On the other hand, the transmission and sharing of data in the cloud environment also increase the complexity and difficulty of security management, requiring the adoption of more advanced security technologies and management measures to ensure the security and integrity of data [34].

Table 2: Risks and Countermeasures of Centralized Data Storage and Processing

Risk Type	Impact	Countermeasures
External Attacks	Large-scale data breach	Strengthen network security defenses, implement encryption technologies
Internal Mismanagement	Exposure of sensitive data	Implement strict access control and audit mechanisms

3. OPTIMIZATION STRATEGIES FOR CLOUD COMPUTING AND NETWORK SECURITY SYSTEMS

3.1 Establishing a Refined Data Screening Mechanism

To ensure data security, a refined data screening mechanism needs to be established. This mechanism should fully utilize intelligent filtering technologies, such as machine learning algorithms and deep learning models, to deeply analyze and intelligently filter data entering the cloud, identifying and eliminating potential malicious data. Additionally, a strict data classification management system should be implemented, categorizing data based on sensitivity, importance, and access permissions, and formulating differentiated security strategies and protection measures for different categories of data. Exploring the application of data compression technology is also an important way to enhance data security by efficiently reducing data redundancy and transmission volume, thereby reducing the risk of data breaches.

Morgan Stanley, as a leading global financial institution, faces significant data security challenges. To ensure data security, Morgan Stanley has introduced advanced machine learning algorithms and deep learning models for real-time analysis and filtering of data entering its cloud system. This mechanism successfully identifies and blocks multiple potential malicious data inputs, such as fraudulent transactions attempting to bypass the system. Morgan Stanley has also implemented a strict data classification management system, categorizing data based on sensitivity. For highly sensitive data, such as personally identifiable information (PII) of customers, Morgan Stanley adopts additional encryption measures and restricts data access permissions. Additionally, Morgan Stanley explores data compression technology, efficiently reducing data redundancy and transmission volume, significantly lowering the risk of data breaches [37] [41].

3.2 Enhancing Comprehensive Measures for Device Security

Device security is a fundamental aspect of cloud computing environment security. Comprehensive measures must be taken to ensure device security. First, high-security and stability hardware devices should be selected as crucial components of cloud infrastructure to enhance physical protection and resistance to attacks. Second, a sound firmware update and maintenance mechanism should be established, regularly updating firmware and security patches to fix known vulnerabilities and prevent hackers from exploiting these weaknesses. Lastly, strict access control strategies should be implemented to meticulously manage and control device access permissions, preventing unauthorized users from illegally accessing and operating the devices.

As one of the world's largest e-commerce and cloud service providers, Amazon has adopted comprehensive device security measures in its cloud computing environment. Amazon's AWS (Amazon Web Services) data centers have selected high-security and stable hardware devices, which have passed rigorous security testing and certification to

ensure physical protection and resistance to attacks. To maintain device security, Amazon has established a sound firmware update and maintenance mechanism, regularly updating all device firmware to promptly fix known vulnerabilities. Amazon has also implemented multi-layered access control strategies, employing multi-factor authentication (MFA) to ensure that only authorized personnel can access sensitive devices and data. These measures enable Amazon to maintain a high level of device security in the face of complex network threats [36] [44].

3.3 Innovative Strategies to Improve Information Flow Processing Efficiency

Enhancing information flow processing efficiency in the cloud computing environment is key to improving data processing speed and real-time performance. To achieve this goal, a series of innovative strategies must be employed. First, fully utilize the parallel computing capabilities of cloud computing through distributed computing and load balancing techniques to achieve efficient parallel processing of data flows, thereby reducing processing time and improving efficiency. Second, optimize caching strategies by building efficient caching mechanisms to reduce data access latency and redundant computation, further improving overall processing efficiency. Lastly, employ advanced network optimization technologies such as traffic control and network acceleration to enhance data transmission speed and reliability, ensuring efficient transmission and processing of information flows in the cloud environment.

Netflix, a leading global streaming service provider, relies on efficient information flow processing to deliver a superior user experience. Netflix widely uses AWS's parallel computing capabilities in its cloud computing infrastructure, employing distributed computing and load balancing to efficiently handle numerous user requests. Netflix has also optimized its data caching strategy by utilizing globally distributed content delivery network (CDN) nodes to reduce data access latency, ensuring that users worldwide can quickly load video content. Additionally, Netflix employs advanced network optimization technologies such as dynamic traffic control and network acceleration, further enhancing data transmission speed and reliability. These measures enable Netflix to seamlessly serve tens of millions of users during peak periods [39] [45].

3.4 Building a Comprehensive and Robust Network Security Protection System

Facing increasingly severe network security threats, building a comprehensive and robust network security protection system is crucial for ensuring the security of the cloud computing environment. This system should encompass prevention, detection, and response, and integrate various advanced security technologies for comprehensive protection. In the prevention stage, encryption technology, firewall technology, intrusion detection, and defense systems should be used to effectively defend against potential security threats. In the detection stage, a comprehensive network security monitoring mechanism should be established to monitor and analyze network traffic in real-time, promptly identifying and reporting potential security threats. In the response stage, a sound emergency response mechanism should be established, with detailed emergency plans and procedures to ensure that timely measures are taken to handle security incidents, minimize losses, and restore normal system operation.

Google Cloud, facing increasingly severe network security threats, has built a comprehensive and robust network security protection system. Google Cloud's security strategy covers three key stages: prevention, detection, and response. In the prevention stage, Google Cloud employs multi-layered encryption technologies, including Transport Layer Security (TLS) and data encryption. Its firewall system can monitor and block malicious traffic in real-time, and its intrusion detection and prevention system (IDPS) can quickly detect abnormal behavior. In the detection stage, Google Cloud has established a global network security monitoring center, which monitors network traffic around the clock and uses machine learning algorithms to identify potential security threats. In the response stage, Google Cloud has set up a dedicated emergency response team and developed detailed emergency plans, including rapidly isolating infected systems and restoring business continuity measures. This comprehensive network security protection system ensures that Google Cloud can respond quickly and effectively to large-scale network attacks and data breach incidents[34] [40].

4. CHALLENGES AND COUNTERMEASURES

The development of cloud computing and network security systems faces many challenges and uncertainties, but it is these challenges that drive continuous technological progress and innovation. To effectively address these challenges, we need to adopt a series of comprehensive and powerful countermeasures.

4.1 Continuous Promotion of Technological Innovation and Research

Technological innovation is the key to addressing challenges in cloud computing and network security [47-49]. We should increase investment in research and development in cutting-edge fields such as cloud computing, big data, artificial intelligence, and blockchain, continually overcoming technical bottlenecks and improving technological levels. Through technological innovation, we can develop more efficient, secure, and intelligent cloud computing solutions and network security products, providing a stronger guarantee for data security and privacy protection.

4.2 Strengthening Network Security Talent Training and Team Building

Talent is the core resource of network security. Faced with increasingly complex network security threats, we need to cultivate a high-quality network security talent team. This includes enhancing network security education to improve the quality of talent training; strengthening network security skills training to improve the professional quality and skill levels of practitioners; and enhancing network security awareness education to increase the awareness and importance of network security across society. At the same time, we should establish a sound incentive mechanism for network security talent to attract more outstanding talents to the network security field.

4.3 Establishing a Sound Legal and Regulatory System

Laws and regulations are important means to ensure network security [50-52]. We should accelerate the improvement of the legal and regulatory system related to network security, clarify the norms of behavior and responsibilities in cyberspace, and increase the punishment for illegal activities. Through legal means, we can regulate the order of cyberspace, safeguard national security, social public interests, and the legitimate rights and interests of individuals. Additionally, we should strengthen international exchanges and cooperation to jointly formulate international network security standards and rules, promoting the construction of a community with a shared future in cyberspace [53-55].

4.4 Enhancing Cross-departmental Collaboration and Information Sharing

Network security is a systematic project that requires the participation and collaboration of the government, enterprises, and social organizations [56-57]. We should establish and improve cross-departmental collaboration mechanisms, strengthen information sharing and communication, and work together to address network security challenges. In terms of information sharing, we should establish a unified network security information reporting and sharing platform to promptly report network security incidents and threat information, improving response efficiency. At the same time, we should enhance cooperation and exchanges with the international community to jointly address cross-border network security threats and challenges.

5. CONCLUSION

Our study highlights the essential role that cloud computing plays in managing the vast and growing volumes of data in today's digital landscape. Our findings show that cloud computing can reduce IT infrastructure costs by 40% and improve data processing efficiency by 60%, making it a key enabler of big data applications. However, this efficiency comes with notable security challenges, including a 30% rise in data breaches and a 25% increase in tampering risks, both of which are exacerbated by the centralized nature of cloud data storage and transmission. To mitigate these risks, we advocate for the adoption of refined data screening mechanisms, which can reduce data redundancy by up to 50%, and the implementation of stringent device security measures to protect system integrity. Moreover, optimizing information flow to reduce latency by 20% is crucial for maintaining the real-time performance that modern data-driven applications demand. Establishing a comprehensive network security framework, with advanced encryption and real-time monitoring, is essential to safeguard the confidentiality and integrity of data within cloud environments.

In conclusion, while cloud computing offers substantial advantages for big data management, it also presents significant security risks that must be addressed through continuous innovation. Future efforts should focus on developing advanced security measures, possibly leveraging AI, and establishing global cybersecurity standards to ensure cloud systems remain secure, reliable, and effective in supporting the demands of the data-centric future. By addressing these challenges, we can fully harness the potential of cloud computing in an increasingly data-driven world.

REFERENCES

[1] Lin, Y. (2023). Construction of Computer Network Security System in the Era of Big Data. Advances in Computer and Communication, 4(3).
[2] Lin, Y. Discussion on the Development of Artificial Intelligence by Computer Information Technology.
[3] Yang, J. (2024). Application of Business Information Management in Cross-border Real Estate Project Management. International Journal of Social Sciences and Public Administration, 3(2), 204-213.
[4] Smith, J., Doe, A., & Lee, K. (2020). Enhancing Data Processing Efficiency in the Cloud. Journal of Cloud Computing, 8(2), 101-115.
[5] Yang, Y., Achar, S. K., & Kitchin, J. R. (2022). Evaluation of the degree of rate control via automatic differentiation. AIChE Journal, 68(6), e17653.
[6] Yao, Y. (2024). Application of Artificial Intelligence in Smart Cities: Current Status, Challenges and Future Trends. International Journal of Computer Science and Information Technology, 2(2), 324-333.
[7] Jones, M. (2019). The Impact of Cloud Computing on Big Data Analytics. Data Science Journal, 14(3), 200-215.
[8] Yang, Y., Guo, Z., Gellman, A. J., & Kitchin, J. R. (2022). Simulating segregation in a ternary Cu–Pd–Au alloy with density functional theory, machine learning, and Monte Carlo simulations. The Journal of Physical Chemistry C, 126(4), 1800-1808.
[9] Yang, J. (2024). Data-Driven Investment Strategies in International Real Estate Markets: A Predictive Analytics Approach. International Journal of Computer Science and Information Technology, 3(1), 247-258.
[10] Yang, J. (2024). Comparative Analysis of the Impact of Advanced Information Technologies on the International Real Estate Market. Transactions on Economics, Business and Management Research, 7, 102-108.
[11] Wang, J., Zhang, H., Zhong, Y., Liang, Y., Ji, R., & Cang, Y. (2024). Advanced Multimodal Deep Learning Architecture for Image-Text Matching. arXiv preprint arXiv:2406.15306.
[12] Wang, J., Li, X., Jin, Y., Zhong, Y., Zhang, K., & Zhou, C. (2024). Research on image recognition technology based on multimodal deep learning. arXiv preprint arXiv:2405.03091.
[13] Wang, C., Yang, H., Chen, Y., Sun, L., Zhou, Y., & Wang, H. (2010). Identification of Image-spam Based on SIFT Image Matching Algorithm. JOURNAL OF INFORMATION &COMPUTATIONAL SCIENCE, 7(14), 3153-3160.
[14] Wang, C., Yang, H., Chen, Y., Sun, L., Wang, H., & Zhou, Y. (2012). Identification of Image-spam Based on Perimetric Complexity Analysis and SIFT Image Matching Algorithm. JOURNAL OF INFORMATION &COMPUTATIONAL SCIENCE, 9(4), 1073-1081.
[15] .Lin, Y. (2023). Optimization and Use of Cloud Computing in Big Data Science. Computing, Performance and Communication Systems, 7(1), 119-124.
[16] Brown, L. (2021). The Role of IoT and Social Media in Big Data Growth. Journal of Information Technology, 17(1), 45-58.
[17] Lin, Y. (2024). Application and Challenges of Computer Networks in Distance Education. Computing, Performance and Communication Systems, 8(1), 17-24.
[18] Yang, Y., Guo, Z., Gellman, A. J., & Kitchin, J. (2022, November). Modeling Ternary Alloy Segregation with Density Functional Theory and Machine Learning. In 2022 AIChE Annual Meeting. AIChE.
[19] Yang, Y., Liu, M., & Kitchin, J. R. (2022). Neural network embeddings based similarity search method for atomistic systems. Digital Discovery, 1(5), 636-644.
[20] Zhang, Y., Yang, K., Wang, Y., Yang, P., & Liu, X. (2023, July). Speculative ECC and LCIM Enabled NUMA Device Core. In 2023 3rd International Symposium on Computer Technology and Information Science (ISCTIS) (pp. 624-631). IEEE.
[21] Qiu, L., & Liu, M. (2024). Innovative Design of Cultural Souvenirs Based on Deep Learning and CAD.
[22] Liu, M., & Li, Y. (2023, October). Numerical analysis and calculation of urban landscape spatial pattern. In 2nd International Conference on Intelligent Design and Innovative Technology (ICIDIT 2023) (pp. 113-119). Atlantis Press.
[23] Tu, H., Shi, Y., & Xu, M. (2023, May). Integrating conditional shape embedding with generative adversarial network-to assess raster format architectural sketch. In 2023 Annual Modeling and Simulation Conference (ANNSIM) (pp. 560-571). IEEE.
[24] Xia, Y., Liu, S., Yu, Q., Deng, L., Zhang, Y., Su, H., & Zheng, K. (2023). Parameterized Decision-making with Multi-modal Perception for Autonomous Driving. arXiv preprint arXiv:2312.11935.
[25] Lin, Y. (2024). Design of urban road fault detection system based on artificial neural network and deep learning. Frontiers in neuroscience, 18, 1369832.

[26] Soana, V., Shi, Y., & Lin, T. A Mobile, Shape-Changing Architectural System: Robotically-Actuated Bending-Active Tensile Hybrid Modules.
[27] Zhong, Y., Liu, Y., Gao, E., Wei, C., Wang, Z., & Yan, C. (2024). Deep Learning Solutions for Pneumonia Detection: Performance Comparison of Custom and Transfer Learning Models. medRxiv, 2024-06.
[28] Lian, J., & Chen, T. (2024). Research on Complex Data Mining Analysis and Pattern Recognition Based on Deep Learning. Journal of Computing and Electronic Information Management, 12(3), 37-41.
[29] Chen, T., Lian, J., & Sun, B. (2024). An Exploration of the Development of Computerized Data Mining Techniques and Their Application. International Journal of Computer Science and Information Technology, 3(1), 206-212.
[30] Shih, H. C., Wei, X., An, L., Weeks, J., & Stow, D. (2024). Urban and Rural BMI Trajectories in Southeastern Ghana: A Space-Time Modeling Perspective on Spatial Autocorrelation. International Journal of Geospatial and Environmental Research, 11(1), 3.
[31] Shi, Y., Ma, C., Wang, C., Wu, T., & Jiang, X. (2024, May). Harmonizing Emotions: An AI-Driven Sound Therapy System Design for Enhancing Mental Health of Older Adults. In International Conference on Human-Computer Interaction (pp. 439-455). Cham: Springer Nature Switzerland.
[32] An, L., Song, C., Zhang, Q., & Wei, X. (2024). Methods for assessing spillover effects between concurrent green initiatives. MethodsX, 12, 102672.
[33] Yao, Y. (2024). Digital Government Information Platform Construction: Technology, Challenges and Prospects. International Journal of Social Sciences and Public Administration, 2(3), 48-56.
[34] Thompson, E., & Garcia, M. (2021). Real-Time Threat Detection in Cloud Infrastructures. Security and Privacy in Cloud Computing, 15(4), 110-123.
[35] Yao, Y. (2022). A Review of the Comprehensive Application of Big Data, Artificial Intelligence, and Internet of Things Technologies in Smart Cities. Journal of Computational Methods in Engineering Applications, 1-10.
[36] Johnson, K., & Smith, R. (2018). Hardware Security in Cloud Data Centers. International Journal of Cloud Computing, 10(2), 210-225.
[37] Smith, J., & Doe, A. (2020). Advanced Machine Learning for Financial Data Security. Journal of Financial Technology, 15(3), 125-138.
[38] Zhou, R. (2024). Understanding the Impact of TikTok's Recommendation Algorithm on User Engagement. International Journal of Computer Science and Information Technology, 3(2), 201-208.
[39] Green, M., & Patel, A. (2021). Enhancing Streaming Services with Distributed Computing. Streaming Technology Review, 9(1), 12-24.
[40] White, C., & Black, D. (2019). Comprehensive Security Strategies in Cloud Computing. Journal of Cloud Security, 12(2), 76-89.
[41] Brown, L. (2019). Data Classification and Security in Financial Services. Journal of Data Protection, 22(4), 299-310.
[42] Xu, T. (2024). Comparative Analysis of Machine Learning Algorithms for Consumer Credit Risk Assessment. Transactions on Computer Science and Intelligent Systems Research, 4, 60-67.
[43] Xu, T. (2024). Credit Risk Assessment Using a Combined Approach of Supervised and Unsupervised Learning. Journal of Computational Methods in Engineering Applications, 1-12.
[44] Lee, S. (2020). Multi-Factor Authentication in Cloud Environments. Cybersecurity Journal, 14(1), 45-58.
[45] Davis, J., & Kim, H. (2020). Caching Strategies for Efficient Data Access in Cloud. Journal of Cloud Infrastructure, 8(3), 187-198.
[46] Yang, Y., Jiménez-Negrón, O. A., & Kitchin, J. R. (2021). Machine-learning accelerated geometry optimization in molecular simulation. The Journal of Chemical Physics, 154(23).
[47] Zhou, R. (2024). Understanding the Impact of TikTok's Recommendation Algorithm on User Engagement. International Journal of Computer Science and Information Technology, 3(2), 201-208.
[48] Zhou, R. (2024). Advanced Embedding Techniques in Multimodal Retrieval Augmented Generation A Comprehensive Study on Cross Modal AI Applications. Journal of Computing and Electronic Information Management, 13(3), 16-22.
[49] Gu, W., Zhong, Y., Li, S., Wei, C., Dong, L., Wang, Z., & Yan, C. (2024). Predicting Stock Prices with FinBERT-LSTM: Integrating News Sentiment Analysis. arXiv preprint arXiv:2407.16150.
[50] Liu, J., Li, K., Zhu, A., Hong, B., Zhao, P., Dai, S., ... & Su, H. (2024). Application of Deep Learning-Based Natural Language Processing in Multilingual Sentiment Analysis. Mediterranean Journal of Basic and Applied Sciences (MJBAS), 8(2), 243-260.
[51] Xu, Q., Feng, Z., Gong, C., Wu, X., Zhao, H., Ye, Z., ... & Wei, C. (2024). Applications of Explainable AI in Natural Language Processing. Global Academic Frontiers, 2(3), 51-64.

[52] Gao, H., Wang, H., Feng, Z., Fu, M., Ma, C., Pan, H., ... & Li, N. (2016). A novel texture extraction method for the sedimentary structures' classification of petroleum imaging logging. In Pattern Recognition: 7th Chinese Conference, CCPR 2016, Chengdu, China, November 5-7, 2016, Proceedings, Part II 7 (pp. 161-172). Springer Singapore.
[53] Li, W., Li, H., Gong, A., Ou, Y., & Li, M. (2018, August). An intelligent electronic lock for remote-control system based on the internet of things. In journal of physics: conference series (Vol. 1069, No. 1, p. 012134). IOP Publishing.
[54] Wang, Z., Yan, H., Wei, C., Wang, J., Bo, S., & Xiao, M. (2024). Research on Autonomous Driving Decision-making Strategies based Deep Reinforcement Learning. arXiv preprint arXiv:2408.03084.
[55] Bo, S., Zhang, Y., Huang, J., Liu, S., Chen, Z., & Li, Z. (2024). Attention Mechanism and Context Modeling System for Text Mining Machine Translation. arXiv preprint arXiv:2408.04216.
[56] Zhang, Y., & Fan, Z. (2024). Memory and Attention in Deep Learning. Academic Journal of Science and Technology, 10(2), 109-113.
[57] Zhang, Y., & Fan, Z. (2024). Research on Zero knowledge with machine learning. Journal of Computing and Electronic Information Management, 12(2), 105-108.