World Journal of Innovation and Modern Technology, Vol. 8, Issue 4, (Apr) 2025
ISSN 2682-5910
DOI: 10.53469/wjimt.2025.08(04).18

Information Security Processing Technology Based on Computer Big Data

Jian Wu

Wuchang Vocational College, Wuhan, Hubei 430200, China

Abstract: ***In the current digital age, the application of computer big data has penetrated into various fields, providing huge business opportunities and growth opportunities for enterprises and organizations. However, with the rapid growth of big data, information security issues have become increasingly prominent, and big data contains a large amount of sensitive information, such as personal identity, financial data, etc. Once leaked or maliciously exploited, it will bring huge risks and losses to individuals and organizations. Therefore, in order to effectively protect the security of big data, improve the credibility and integrity of data, it is particularly important to explore information security processing technologies for computer big data. Therefore, this article mainly explores the application of information security processing technology in computer big data, and provides reference for improving the effectiveness of information security processing in computer big data.***

Keywords: Computer; Big data; Information security; Processing technology; Application Analysis.

1. PREFACE

With the rapid development of big data technology, the application scope of big data is becoming more and more extensive, and the amount and complexity of data involved are also increasing. However, with the increase of data scale, information security issues have become more important and complex. The information security processing in big data involves protecting the confidentiality, integrity, and availability of data, as well as preventing malicious attacks and data leaks. Due to the characteristics of big data, traditional information security processing methods are no longer applicable, and new technologies need to be researched and explored to address these challenges. By exploring the information security processing technology of computer big data, we can better protect the security and privacy of big data, provide reliable guarantees for the application of big data, and also provide reference and guidance for related research and practice. Xie et al. [1] introduced RTop-K, an ultra-fast row-wise top-K selection algorithm for GPU-accelerated neural network computations. In healthcare applications, Lin et al. [2] investigated intelligent physical exercise monitoring for improving executive function in children with ADHD, while Peng et al. [3] examined the impact of aerobic exercise intensity on cognitive function and sleep patterns. Logistics optimization has seen significant innovation through Luo et al. [4], who developed a novel path planning algorithm combining transformer and GCN networks for intelligent logistics robots. Customer experience and human-computer interaction have been enhanced through several studies. Xu et al. [5] designed experience management tools based on customer perceived value in the electric vehicle market, and Shan et al. [6] conducted a cross-cultural analysis of large language models' implications. Clinical AI applications have progressed with Shen et al. [7] developing an LSTM-based system for anesthetic dose management in cancer surgery. Cybersecurity and financial applications of AI have also seen notable developments. Xu et al. [8] analyzed adversarial machine learning attacks and defenses in cybersecurity, while Chew et al. [9] created an AI-optimized model for e-commerce accounting data integration and financial risk assessment. Finally, Wang et al. [10] contributed to autonomous vehicle technology with their end-to-end AI driving system.

2. THE IMPORTANCE OF INFORMATION SECURITY PROCESSING TECHNOLOGY APPLICATION IN COMPUTER BIG DATA

Firstly, big data contains a large amount of sensitive personal information, such as personal identity and financial data. By selecting appropriate information security processing techniques, technicians can effectively protect this information and prevent it from being maliciously exploited.

Secondly, big data stores important data for enterprises and organizations, such as trade secrets and user information. Information security processing technologies can prevent hacker attacks and data breaches, protecting enterprises and users from losses. In addition, the value of big data lies in its accuracy and credibility. Information security processing technology can ensure the integrity of data, prevent data from being tampered with

or forged, and ensure the reliability and credibility of data. Meanwhile, with the strengthening of data protection and privacy laws, organizations need to comply with relevant compliance requirements, and information security processing technologies can help organizations meet legal requirements and reduce the risk of violations.

Finally, the analysis and sharing of big data are crucial for decision-making and innovation in organizations and society. Information security processing technologies can provide controllable ways of data sharing and analysis, protecting the privacy and security of data.

3. PROBLEMS IN THE APPLICATION OF INFORMATION SECURITY PROCESSING TECHNOLOGY FOR COMPUTER BIG DATA

3.1 Processing speed and large data volume

Computer big data usually contains massive amounts of information, and its secure processing requires high computing and processing capabilities. However, information security processing technology may face problems such as slow processing speed and long response time when dealing with big data, which can affect the performance and efficiency of the system.

3.2 Complex data formats and structures

At present, big data typically involves multiple data formats and structures, such as structured data, semi-structured data, and unstructured data. Information security processing technology needs to adapt to different data formats and structures to ensure consistency and effectiveness in secure processing across different types of data.

3.3 Balancing Privacy Protection and Data Analysis Requirements

When conducting information security processing for big data, it is necessary to balance the relationship between privacy protection and data analysis requirements. On the one hand, privacy protection requires restricting the access and use of data to protect users' personal privacy; On the other hand, data analysis requires the full utilization of data to mine useful information. How to achieve effective analysis and utilization of data while protecting privacy is a problem that needs to be solved.

3.4 Technical updates and vulnerability fixes

The information security processing technology of computer big data needs to keep pace with constantly developing technologies and threats. With the advancement of technology, new security vulnerabilities and threats may emerge, posing new challenges to existing information security processing technologies. Therefore, it is very important for technicians to update and fix technical vulnerabilities in a timely manner, and maintain the effectiveness and reliability of information security processing technology.

4. APPLICATION ANALYSIS OF INFORMATION SECURITY PROCESSING TECHNOLOGY FOR COMPUTER BIG DATA

4.1 Data Protection and Encryption

4.1.1 Data Encryption:

Data encryption is a commonly used data protection technique that encrypts data into a seemingly meaningless string of characters, which can only be decrypted and restored to the original data by someone with the correct key. Meanwhile, encryption renders the stolen data meaningless to attackers, thereby protecting the confidentiality of sensitive information.

4.1.2 Data Desensitization:

Data anonymization is the process of processing sensitive data to protect privacy and comply with data protection regulations. Data anonymization technology can process some information of sensitive data through replacement,

deletion, blocking, etc., so that sensitive information cannot be identified. This can protect the confidentiality of data while preserving its integrity and availability.

4.1.3 Key Management:

In data encryption, the key is the key to ensuring data security, and key management technology involves the management of key generation, distribution, storage, and updates. Reasonable key management can ensure the security of keys, prevent key leakage and abuse, and thus protect the security of encrypted data.

4.1.4 Access Control and Permission Management:

Data protection also requires access control and permission management to restrict access and use of sensitive data. Access control and permission management technologies can authenticate, authorize, and audit users to ensure that only legitimate users can access and use sensitive data. At the same time, data access behavior can be monitored and audited to promptly detect and prevent unauthorized access.

4.2 Anomaly detection and threat identification

Firstly, anomaly detection: Anomaly detection is a technique that identifies data points or events that do not conform to normal patterns through statistical analysis and modeling of data. In the big data environment, technicians can use machine learning, statistical analysis, and data mining techniques to analyze large-scale data and discover abnormal behaviors. For example, by monitoring network traffic, abnormal behaviors such as network intrusion and malicious attacks can be detected.

Secondly, threat identification: Threat identification refers to the analysis and detection of information in big data to discover and identify potential security threats. It can identify and match known threats by establishing a threat intelligence database, as well as detect and identify unknown threats through techniques such as behavior analysis and pattern recognition. Threat identification can help detect and respond to potential attacks and security threats early on. At the same time, real-time monitoring and response: In the big data environment, anomaly detection and threat identification need to have real-time capabilities, able to monitor and respond to large-scale data in real time. By utilizing distributed computing and real-time data processing technology, technicians can monitor big data in real time, detect and respond to abnormal behaviors and threats in a timely manner.

Finally, integrating other security technologies: anomaly detection and threat identification need to be integrated with other security technologies to enhance the ability of security protection. For example, anomaly detection can be integrated with security devices such as firewalls and intrusion detection systems (IDS) to achieve multi-level security protection and threat identification [2].

4.3 Data Traceability and Tracking

4.3.1 Data Traceability:

Data traceability refers to the process of tracking and recording the flow of data in big data, determining the source and direction of data. By establishing a data flow control system, technicians can monitor and record the generation, transmission, storage, and access of data to achieve full traceability of data. Data traceability can help quickly locate the source of data leakage and abuse, trace responsibility, and supervise the compliant use of data.

4.3.2 Data Tracking:

Data tracking refers to tracking and monitoring the flow and operation of data in big data, and tracking the real-time flow and usage of data. Technicians can achieve real-time tracking and monitoring of data through techniques such as operation logs, access records, and behavior analysis. Data tracking can help detect violations such as data abuse, theft, and tampering in a timely manner, improving the ability to protect data security and privacy.

4.3.3 Real time alarm and response:

Data traceability and tracking require real-time monitoring and response to large-scale data. By establishing a real-time alarm system to monitor abnormal data flow and operations, once abnormal situations are detected, alarm signals can be promptly issued and corresponding response measures can be taken. Real time alerts and responses can help quickly detect and respond to data breaches, abuse, and violations.

4.3.4 Privacy Protection and Compliance:

Data traceability and tracing need to be combined with privacy protection and compliance requirements. In the process of data tracking, technicians need to take measures to protect the privacy of sensitive data and prevent personal privacy information from being abused and leaked. At the same time, it is also necessary to ensure the compliance of data tracking, comply with relevant laws and regulations, and privacy protection policies.

4.4 Security Compliance and Audit

4.4.1 Safety compliance monitoring:

Security compliance monitoring refers to monitoring and evaluating the security policies, access controls, data encryption, and other security mechanisms of big data systems to ensure their compliance. By monitoring and analyzing the security status of the system in real-time, security vulnerabilities, abnormal behaviors, and attack behaviors can be detected and prevented in a timely manner, ensuring the security compliance of the system and complying with relevant laws, regulations, and industry standards.

4.4.2 Security Audit:

Security audit refers to the logging and auditing of big data systems and data operations to track and monitor the usage and operation of data. By means of operation logs, access records, and behavior auditing of the system, full monitoring and auditing of data can be achieved. Security auditing can help identify violations such as data abuse, theft, and tampering, protecting the security and privacy of data.

4.4.3 Compliance Report:

Compliance report refers to the regular compliance assessment and reporting of big data systems and data operations to demonstrate the compliance of the systems and data. By collecting and analyzing security logs and operational records of the system, compliance reports can be generated, including evaluation results on system security status, access control, data protection, and privacy protection. Compliance reports can serve as a basis for evaluating and monitoring data security, helping businesses and organizations ensure data security and compliance.

4.4.3 Security Compliance Strategy:

Security compliance and auditing require the establishment of corresponding security compliance policies, including requirements for security standards, permission management, data encryption, and privacy protection. By formulating and implementing security and compliance policies, the security and compliance of big data systems and data operations can be ensured.

4.5 Prediction and Warning

4.5.1 Threat Prediction:

Technicians can predict potential security threats by analyzing and modeling security events, attack behaviors, and abnormal behaviors in big data systems. And by utilizing machine learning, data mining, and statistical analysis techniques, patterns and patterns related to security threats can be discovered and identified. By analyzing and predicting these patterns and patterns, early warning and corresponding protective measures can be taken to avoid the occurrence of security incidents.

4.5.2 Abnormal detection:

Technicians can discover abnormal behaviors and events by analyzing behavioral data in big data systems. By establishing baseline models and behavioral feature models, abnormal behaviors that do not conform to normal behavior can be identified. By detecting and analyzing these abnormal behaviors, early warning and corresponding measures can be taken to prevent the occurrence or expansion of security incidents.

4.5.3 Real time monitoring:

Technicians can detect and respond to security incidents in a timely manner through real-time monitoring of big data systems. By analyzing and processing the real-time data streams of the system, they can monitor network traffic, access logs, and abnormal behavior in real-time. Through real-time monitoring, security threats in the system can be detected and alerted in a timely manner, and corresponding measures can be taken to protect the security of the system and data.

4.5.4 Intelligent Warning:

By combining big data processing and artificial intelligence technology, an intelligent warning system can be achieved. By conducting real-time analysis and learning of security events and threats in big data systems, intelligent warning models can be established. Through these models, potential security threats can be automatically identified and predicted, and corresponding warning notifications can be issued. Intelligent warning systems can greatly improve the detection and response efficiency of security incidents, helping enterprises and organizations better protect the security of systems and data.

5. CONCLUSION

In summary, with the increase of data volume, processing speed and efficiency have become key issues, and privacy protection and data integrity verification are still difficult problems that need further research and improvement. At the same time, emerging technologies and attack methods also pose new threats to information security. Technical personnel need to continue to conduct in-depth research and exploration of information security processing technologies for computer big data, including improving existing technologies, developing new security algorithms and protocols, and strengthening the detection and prevention of malicious attacks. At the same time, it is necessary to strengthen interdisciplinary cooperation, integrate knowledge from fields such as computer science, mathematics, statistics, etc., and jointly promote the development of information security processing technology. Through continuous exploration and innovation, effective solutions can be provided for the security and privacy protection of big data, promoting the sustainable development of big data.

REFERENCES

[1] Xie, X., Luo, Y., Peng, H., & Ding, C. RTop-K: Ultra-Fast Row-Wise Top-K Selection for Neural Network Acceleration on GPUs. In The Thirteenth International Conference on Learning Representations.
[2] Lin, L., Li, N., & Zhao, S. (2025). The effect of intelligent monitoring of physical exercise on executive function in children with ADHD. Alexandria Engineering Journal, 122, 355-363.
[3] Peng, Y., Zhang, G., & Pang, H. (2025). Impact of Short-Duration Aerobic Exercise Intensity on Executive Function and Sleep. arXiv preprint arXiv:2503.09077.
[4] Luo, H., Wei, J., Zhao, S., Liang, A., Xu, Z., & Jiang, R. (2024). Intelligent logistics management robot path planning algorithm integrating transformer and gcn network. IECE Transactions on Internet of Things, 2(4), 95-112.
[5] Xu, Y., Shan, X., Guo, M., Gao, W., & Lin, Y. S. (2024). Design and application of experience management tools from the perspective of customer perceived value: A study on the electric vehicle market. World Electric Vehicle Journal, 15(8), 378.
[6] Shan, X., Xu, Y., Wang, Y., Lin, Y. S., & Bao, Y. (2024, June). Cross-Cultural Implications of Large Language Models: An Extended Comparative Analysis. In International Conference on Human-Computer Interaction (pp. 106-118). Cham: Springer Nature Switzerland.
[7] Shen, Z., Wang, Y., Hu, K., Wang, Z., & Lin, S. (2025). Exploration of Clinical Application of AI System Incorporating LSTM Algorithm for Management of Anesthetic Dose in Cancer Surgery. Journal of Theory and Practice in Clinical Sciences, 2, 17-28.
[8] Xu, J., Wang, Y., Chen, H., & Shen, Z. (2025). Adversarial Machine Learning in Cybersecurity: Attacks and Defenses. International Journal of Management Science Research, 8(2), 26-33.

[9] Chew, J., Shen, Z., Hu, K., Wang, Y., & Wang, Z. (2025). Artificial Intelligence Optimizes the Accounting Data Integration and Financial Risk Assessment Model of the E-commerce Platform. International Journal of Management Science Research, 8(2), 7-17.
[10] Wang, Y., Shen, Z., Hu, K., Yang, J., & Li, C. (2025). AI End-to-End Autonomous Driving.