Journal of Electronics and Information Science (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2025.100202
ISSN 2371-9524 Vol. 10 Num. 2

Artificial Intelligence Data Security Evaluation in Big Data Cloud Computing Environment

Hui Chen[1,a,*], Hua Yuan[1,b]

[1]*The 15th Research Institute of China Electronics Technology Group Corporation, Beijing, China*
[a]*chenhui2751@163.com*, [b]*yuanhua750@163.com*
[*]*Corresponding author*

Keywords: Artificial Intelligence, Data Security, Big Data, Cloud Computing

Abstract: With the increasing popularity of network technology and information concepts, Big Data (BD) and cloud computing technologies have emerged and are widely used in all industries. BD technology can fully utilize the application value of information. Cloud computing can store a large amount of data, and improve data usage efficiency, so as to make full use of the value of data. At the same time, data security issues have become increasingly important. However, due to various factors, many users are faced with data breaches and privacy violations in the BD cloud computing environment. In this case, there are some data security risks, and the key issue is to consider how to avoid these risks. By analyzing the relationship and differences between BD and cloud computing, this article studied the issues and influencing factors of Artificial Intelligence (AI) data security in the BD cloud computing environment, and proposed corresponding optimization strategies, so as to improve data security and provide users with a brand new experience. Through comparison, it could be seen that the data processing speed and legal integrity after using the optimization strategy significantly improved. Among them, data processing speed increased by 7.2% and legal integrity increased by 10.4%. BD cloud computing could effectively improve AI data security performance.

1. Introduction

1.1 Investigation Background

The acquisition and storage of network information primarily depend on storage devices for data transmission. With the advancement of information technology, new data storage solutions have emerged through Big Data applications and information development techniques. However, the complex and ever-evolving network environment introduces security risks to data. In practical applications of large-scale databases, security vulnerabilities emerge due to the distributed and open nature of Big Data. Consequently, ensuring data reliability and security in Big Data cloud environments remains a critical challenge in contemporary research.

1.2 Literature Review of Data Security

Data security has always been a key concern. Data security is a data centric stance that focuses on the security and compliance of data throughout its lifecycle, especially sensitive data. Esposito Christian studied the potential of using blockchain technology to protect healthcare data hosted in the cloud, and described the practical challenges of this proposition and the further research needed [1]. Isaak Jim believed that users' personally identifiable information should be protected by the platform, and a comprehensive privacy policy law should be implemented [2]. Abouelmehdi Karim investigated the most advanced security and privacy challenges faced by BD in the healthcare industry. He evaluated how security and privacy issues arose in the context of large healthcare data, and discussed ways to address these issues [3]. Salman Tara investigated several blockchain based approaches to security services. These services included authentication, confidentiality, privacy and access control lists, data and resource sources, and integrity assurance [4]. Xiao Liang studied attack models for Internet of Things(IoT) systems and tested IoT security solutions based on machine learning. He also discussed the challenges of implementing these machine learning based security solutions in IoT systems [5]. Lu Yunlong developed a blockchain based secure data exchange architecture for distributed parties. Combining collaborative learning and data protection, it described the data sharing problem as a machine learning problem [6]. Taylor Paul J conducted a systematic analysis of the most commonly used blockchain security applications, and also clarified the future research, education, and practice directions in the field of blockchain and network security [7]. The above studies all described the importance of data security, but they were not analyzed in conjunction with BD.

1.3 Literature Review on the Application of BD and Cloud Computing in Data Security

The network environment under BD cloud computing is complex and volatile, and its potential risks would affect the safe transmission and storage of data. BD and cloud computing have contributes significantly in AI data security. Lo'ai A. Tawalbeh introduced the existing layered cloud architecture and proposed a solution to solve BD storage. Secondly, he explored the use of cloud systems for BD processing and analysis [8]. In order to establish a comprehensive risk assessment methodology, Sharma Abhishek conducted an extensive literature review to identify risk factors that might affect cloud computing adoption [9]. Ray Soumya studied the potential security threats of different BD computing technologies and proposed a defense mechanism to alleviate these potential security threats. In order to identify security issues, thorough analysis and observation were conducted on different existing BD systems [10]. Shakya Subarana provided data security analysis and solutions for privacy protection frameworks during data migration. He established a secure socket layer and introduced a migration ticket with minimum permissions [11]. Bai Xiang evaluated models for retaining and heterogeneous data. He provided a visual explanation of the decisions made by the model and analyzed the trade-offs between model performance and communication costs during joint training [12]. The above studies all described the application of BD and cloud computing in data security, but there were still some shortcomings in data security optimization.

1.4 Investigation Significance and Innovation

In order to study the security issues of AI data in the BD cloud computing environment, this paper analyzed the security thresholds and risk eigenvalues of AI data security through machine learning. In the experimental part, the data privacy protection and data security supervision in the BD cloud computing environment were analyzed. Through experimental analysis, it was found that

the optimized data security strategy could effectively improve data security protection and supervision. Compared with other literature, this article focused on comparative analysis of the regulatory and privacy protection effects of data security.

2. Evaluation of the Relationship and Differences between BD and Cloud Computing

2.1 Evaluation of the Relationship between BD and Cloud Computing

In the BD cloud computing environment, BD and cloud computing provide data sources and data management tools. BD integrates massive amounts of data and combines high-speed data streams with multiple internal data types that can be used as data sources. Cloud computing is becoming one of the most useful and intelligent technologies in the field of network security [13]. By supporting intelligent logic and computing algorithms, as well as advanced network transmission capabilities, cloud computing can display, calculate, and decompose all information in a data source in a short time. Considering the huge data sources, cloud computing technology first breaks down all the information in the data source into parts based on current network and bandwidth resources, and then rationally allocates it to multiple computers running at the same time to achieve efficient computing and understand the relationship between different data and information, so as to finally combine all calculations to use the data source for computing. Effective data processing requires professional technical support, so real-time BD analysis is used to allocate tasks between multiple computers that require distributed processing. Facts have proven that there is a close connection between BD and cloud computing. Users must understand the relationship between them and their functional positioning in the application process to improve data utilization and meet the needs of different data applications such as distributed storage of BD.

2.2 Evaluation of the Differences between BD Cloud Computing and Traditional Data Management Models

Data privacy is one of the interesting topics on websites [14]. Compared to traditional data management methods, BD cloud computing has irreplaceable advantages, with the following main differences. First, BD cloud computing provides faster data processing speed. Cloud service platform applications can process information and improve overall computer performance in the era of BD. In the past, information processing was fast, but utilization was reduced, thus wasting resources in practical operations. However, using BD cloud computing can effectively improve data processing speed and quickly achieve data classification and analysis. Second, BD cloud computing has strong processing capabilities and low costs. Unlike existing data processing technologies, BD cloud computing integrates all data and information onto a single system platform, thus integrating the latest data network technology to facilitate the actual processing of user information, thereby breaking the restrictions on original resources and improving the efficiency of resource search.

Third, BD cloud computing provides convenient access and management. BD cloud computing connects all data resources through virtual technology. Users do not need to consider the impact of time when searching for data resources, but directly search for information resources. In real resource requests, users can freely use resources using existing virtual technology platforms. In addition, the required resources can be obtained without worrying about the source of resource information. Access to resource information at any time can simplify the work of users. Fourth, a flexible BD cloud computing platform. After the Internet is turned on, access can only be made using the correct login password. Therefore, in the practical application of BD cloud computing platform, it can reduce the demand for computers and improve their use efficiency.

2.3 Evaluation of the Role of Data Security in the BD Cloud Computing Environment

Data security in the cloud data environment has become increasingly important, which not only has a negative impact on the development of science and technology, but also has a negative impact on the popularity of computer network technology. Due to the late application of computer network technology, there is currently no comprehensive network security protection mechanism to support it. BD cloud computing is an existing computing and distributed technology that is vulnerable to attacks. BD cloud computing is based on the combination of new computing technologies such as distributed processing. It has powerful arithmetic functions, which can filter and analyze large amounts of data and provide people with powerful functionality and scalability. In this case, combined with traditional computer technology, dynamic computing capabilities have been formed. Only by updating and improving BD cloud computing technology and improving the quality of security management can data security in the cloud computing BD environment be improved.

3. Evaluation of Issues and Influencing Factors of AI Data Security

3.1 Evaluation of AI Data Security Issues

The problem of AI data security is mainly reflected in the following aspects, as shown in Figure 1.

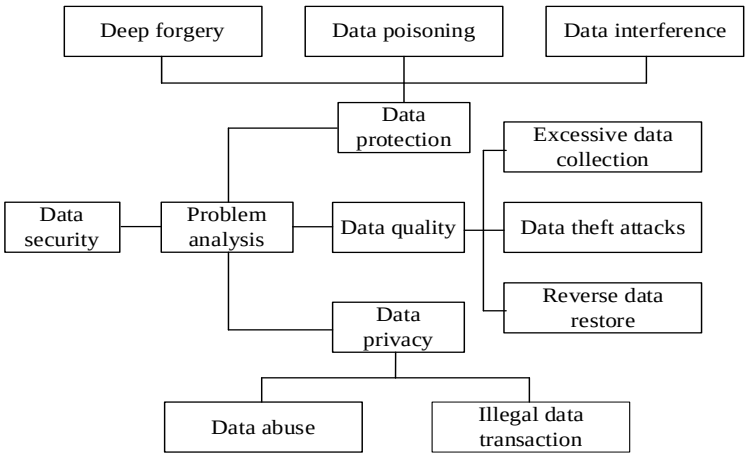


Figure 1 Analysis of AI data security issues

3.1.1 Data Quality and Safety Issues

Data is a bridge between physical space and virtual space. If there is a problem with data quality, it cannot reflect reality. AI models built on this basis are prone to skewed or erroneous predictions. The security risk of AI data quality refers to the risk of data quality loss resulting from incorrect decision-making of algorithm models through direct or indirect attacks on learning data. Data poisoning is a direct attack by attackers on learning data samples, thus allowing AI to contaminate learning data and study error information to change classification restrictions. AI must collect target information through an execution feedback mechanism, so attackers use the model feedback mechanism to directly write inaccurate data into the model or scramble data, thus misleading AI to make decisions. Deep forgery refers to the simulation of pseudo realistic digital images of specific objects through sound and video. Deep forgery technology itself is neutral, but malicious exploitation can trigger a crisis of social trust.

3.1.2 Data Privacy Security Issues

Data collection is the first step in the data lifecycle and the key to the development of AI. Data collection must follow the minimum principle and require the consent of the collected user. Excessive data collection means collecting data in violation of this principle, so excessive collection of personal data is not allowed. Currently, due to the popularity of intelligent devices, various intelligent applications often force users to read their personal data. Even if users work secretly in the background, they would collect data unrelated to services. User data is usually controlled by software developers or operators, and there is a serious imbalance between the two [15]. Therefore, users in cyberspace have become "transparent people ", the ultimate purpose and use of excessive data collection are themselves unknown, and the rights to personal information, privacy, and data have been seriously violated. If intermediate or simulated results are used to extract important information from learning data and steal learning data, an AI data theft attack can occur. Attackers access the model application interface through technologies such as data display and inference, and reverse restore the user's data privacy information based on their specific mapping relationships. In addition, attackers can access the software interface of the model, and guess model parameters, architecture, hyperparameters, and other information, or build models with similar functions to steal data information from the model.

3.1.3 Data Protection Security Issues

When generating and creating, recording and transmitting, processing and using data, data generates the power to dominate and control people, that is, the power of data driven by different interests. The growth of data power has led to the alienation of data power, thus resulting in data abuse, privatization of platform power, and other phenomena. In the process of personal data marketing, there are more disputes related to data protection, and the issue of data ownership is the core of data rights disputes. In the marketing process, the core issue between data developers and users, as well as between data developers and data developers, is personal data usage disputes. An effective balance must be achieved between the interests of data developers and users and the public interest. Data abuse refers to the misuse of data or the use of personal data or databases in unknown ways without the informed consent of the data subject. Driven by value advantages, in the use of data resources, there have emerged a black and gray profit chain of data over rights, over protocol analysis, and even generated for illegal data transactions, thus causing significant damage to personal privacy, trade secrets, and national security.

3.2 Evaluation of Factors Affecting AI Data Security

The main factors affecting AI data security are as follows, as shown in Figure 2. The first is that individual users have little understanding of data security and privacy protection. There is no need to decide to register for a network platform account, browse irregular websites, or download software without verification. Users illegally steal or sell information from others for personal purposes, and intentionally or unintentionally disseminate information about personal data protection. The second is that enterprises do not attach importance to the security and confidentiality of user data. The organization's data security management system is incomplete and cannot adapt to the constantly changing environment of user privacy applications. Employees' data security and privacy processes or systems cannot monitor each other. For example, the information collected by the company is also arbitrarily obtained by other cooperative organizations and sold to illegal persons. The third is that the laws on data security and the protection of citizens' personal data are not perfect. The law is the most important guarantee for data security and the protection of

citizens. However, when formulating a legal system, the state only focuses on solving the current privacy and security issues of citizens. There are no time constraints, and complex and diverse network environments and information leaks are not considered. In the era of AI, due to the complexity and variability of data usage and personal data exchange, it is neither relevant nor applicable. Without these conditions, sustainable and effective protection cannot be achieved. The fourth is that regulation cannot keep up with technological progress, thus resulting in technological anomalies that pose a potential threat to security and data protection. AI focuses more on data correlation rather than causal relationships. Neural network algorithms are very complex. When they get out of control, people simply cannot understand the internal working mechanism.

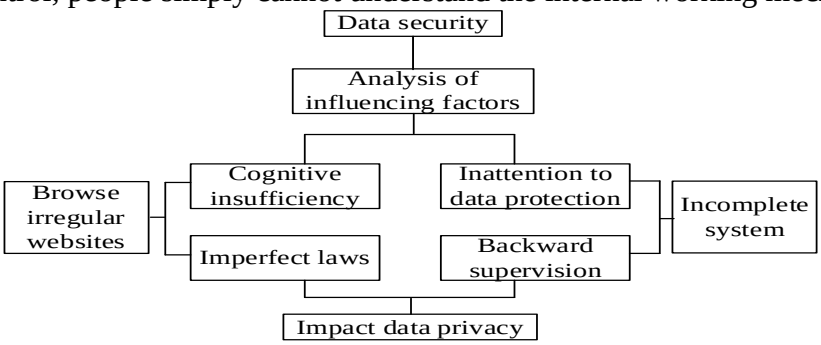


Figure 2 Factors affecting AI data security

4. Application of Machine Learning in AI Data Security

In order to study AI data security under BD and cloud computing, this paper studied the storage model of AI data security through machine learning. It studied the distribution feature information entropy of AI data security, and finally obtained data risk feature information and data security threshold function. Firstly, this article investigated the storage state model of AI data as follows:

$$\begin{pmatrix} A \\ P(A) \end{pmatrix} = \begin{Bmatrix} b_1, b_2, \cdots, b_m \\ p(b_1), p(b_2), \cdots, p(b_m) \end{Bmatrix} \tag{1}$$

Among them, b_m is the transmission sequence of AI data, and $p(b_m)$ is the sequence feature distribution of AI data. A is AI data. Next, the distribution feature information entropy of AI data security under BD is studied as follows:

$$S(A) = -\sum_{i=1}^{m} p(b_i) \log_2 p(b_i) \tag{2}$$

Among them, $p(b_i)$ is the association rule for AI data. Next, the risk characteristic values of AI data in the cloud computing environment are analyzed as follows:

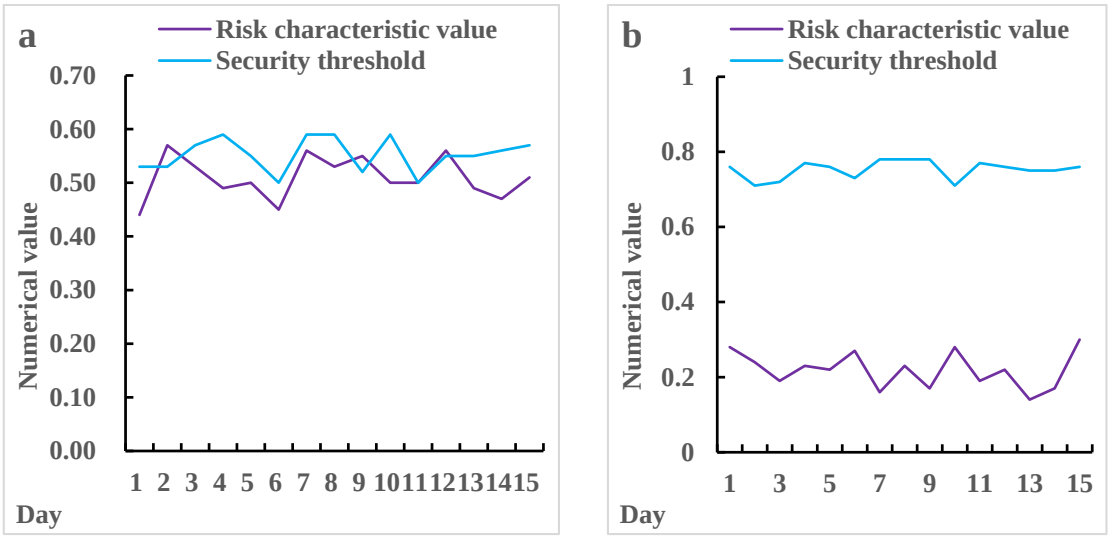
$$R_1(m,n) = \sum_{i=1}^{N} r_i e^{j\delta(m-n)} \tag{3}$$

Among them, r_i is the risk factor of AI data; e is the risk decision factor of AI data; m and n are the maximum and minimum risk values of the data, respectively. Finally, the security threshold function for AI data can be obtained as follows:

$$Y = (m-n) \log_2 [r_{i1}, r_{i2}, \cdots, r_{in}] / R_1(m,n) \tag{4}$$

Since the scoring of risk eigenvalues and security thresholds is related to the security issues of AI

data in different environments, the risk eigenvalues and security threshold functions of AI data are studied based on machine learning algorithms to investigate the AI data security of an enterprise in different environments. The comprehensive score of its risk characteristic value and safety threshold was 1, and a total of 15 days of data were investigated. The specific investigation results are shown in Figure 3.



a: AI data in traditional environments b: AI data under BD cloud computing

Figure 3 Risk characteristic values and security thresholds for AI data security in different environments

Figure 3a showed AI data in a traditional environment. During the fifteen days of this investigation, the risk characteristic value of the enterprise stabilized between 0.4 and 0.6. The lowest risk characteristic value was 0.44, and the highest risk characteristic value was 0.57. This indicated that there were certain security risks associated with data in traditional environments, which caused difficulties in data transmission and processing. In addition, in the survey, its safety threshold was between 0.5 and 0.6, with the highest safety threshold being only 0.59. This indicated that the data information infrastructure in traditional environments was not perfect enough and there were also data isolation issues in the storage and sharing of data.

Figure 3b showed AI data under BD cloud computing. The enterprise's AI data security risk characteristic value under BD cloud computing significantly decreased, and its range was between 0.1 and 0.3. This was far lower than the security risk value of traditional environments, and also confirmed that the defense of AI data under BD cloud computing was more complete. Various data attack issues could be applied to reduce their security risk value. The survey data showed that the AI data security threshold in this environment also significantly improved, with a range of 0.7 to 0.8.Compared to the traditional security threshold, it increased by 0.2. These all demonstrated that the BD cloud computing environment was more secure, which facilitated data storage and transmission, and also improved the security of data collection.

5. Evaluation of AI Data Security and Privacy Issues in the BD Cloud Computing Environment

Cloud computing is used to store BD. Through operations such as data extraction, analysis, and calculation, the value of data can be fully utilized. Data security includes security and privacy throughout the cloud lifecycle. This is mainly about the security of user data and personal information privacy on cloud platforms. The security, integrity, and availability of data face many

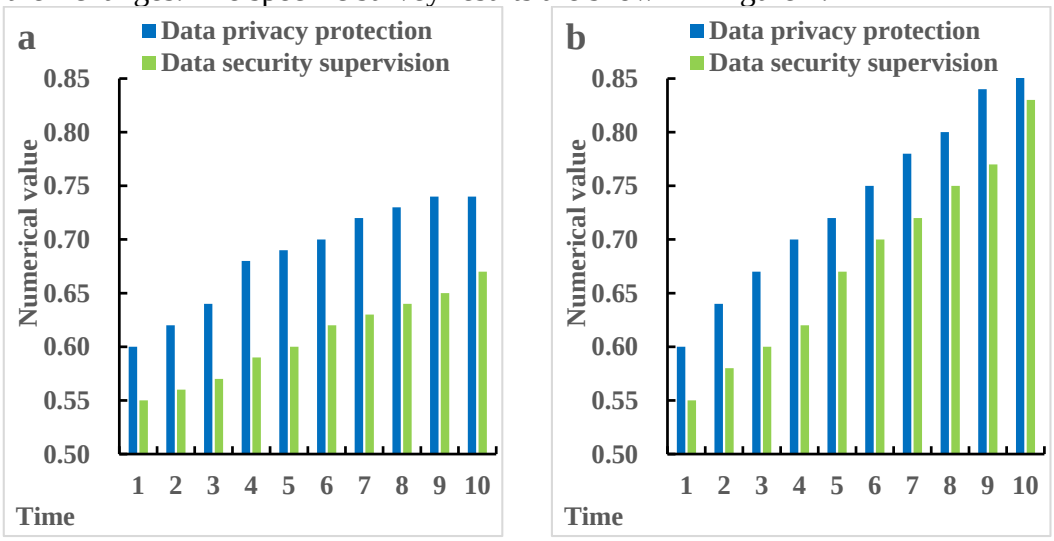
challenges, and the effectiveness of existing algorithmic security protocols has been weakened. Cloud platform data security mainly includes monitoring user behavior, user data operations, verifying the reliability of the cloud platform, and verifying whether the download mechanism is safe and reasonable. If the authenticity of cloud platform providers and user information abuse cannot be protected, external regulatory agencies or competent government agencies should be established.

BD applications are expanding in various industries, and the security and privacy issues of BD are also growing. When collecting and summarizing user's personal behavior data, there is a problem of infringing personal information. In addition to data protection and security, employee status and behavior can also have unsafe effects on data. BD sharing and comfortable use are privacy and security issues that cannot be ignored. In the era of AI, personal data is easily leaked due to various violations of economic interests or other reasons. Data science and technology use analysis of lost data to improve and retrieve leaked data for accurate advertising marketing. Therefore, controlling the use of BD is very important, including managing access to BD and restricting the behavior of user roles. When using BD, unless they can be effectively identified, they are considered unreliable. Criminals can falsify data, thus leading to analysis errors.

6. Experimental Evaluation of Data Security under BD Cloud Computing

6.1 Evaluation of Privacy Protection and Security Supervision of AI Data in Different Environments

Based on the privacy issues of AI data security under BD cloud computing studied above, it is found that AI data can be exposed or abused for various reasons in different environments, which seriously affects the security and privacy of data. This article also analyzes and studies the privacy protection and security supervision of AI data in different environments. The initial value for data privacy protection was 0.60, and the initial value for data security supervision was 0.55. The total value of these two indicators was 1. The changes of these two indicators over time in different environments were investigated for a total of ten days, and comprehensive analysis was conducted based on their changes. The specific survey results are shown in Figure 4.



a: AI data in traditional environments b: AI data under BD cloud computing

Figure 4 Data privacy protection and data security supervision in different environments

Figure 4a showed AI data in a traditional environment. Data privacy protection increased to 0.74

on the tenth day, with the entire process increasing by 0.14. Data security supervision increased to 0.67 on the 10th day, with an increase of 0.12 during the entire process. This indicated that the effectiveness of AI data privacy protection and security supervision was slowly improving in traditional environments, but the increase was very slow. Figure 4b showed AI data under BD cloud computing. The growth rate of data privacy protection and data security supervision in BD cloud computing was higher than in traditional environments. Among them, data privacy protection improved by 0.05 compared to traditional environments, and data security supervision improved by 0.07 compared to traditional environments. It could be seen that BD cloud computing could effectively improve the effectiveness of data privacy protection. At the same time, the security supervision of the platform in the BD cloud computing environment was also higher than that in traditional environments.

6.2 Evaluation of Public Satisfaction with AI Data Security

Data security issues require improving data protection systems and improving data encryption technology to effectively ensure data security. Therefore, data security also requires optimizing data security protection strategies based on public feedback by investigating the satisfaction of the public with data security under BD cloud computing. To this end, this article investigated the satisfaction of people in three cities with AI data security under BD cloud computing, with 50 people surveyed in each city. The survey level was divided into three levels: safe, general, and unsafe. The specific survey results are shown in Table 1.

Table 1 Satisfactory effects of three regions on AI data security under BD cloud computing

	Safe	Common	Unsafe
City 1	40	7	3
City 2	45	4	1
City 3	43	4	3
Total	128	15	7

According to the data depicted in Table 1, people in the three cities were relatively satisfied with AI data security under BD cloud computing. Among the people who believed in safety, the number of people in City 2 was the largest, accounting for 35.2% of this group; among the general population, City 1 had the largest number of people, accounting for 46.7% of this group; among the people who believed that they were unsafe, Cities 1 and 3 accounted for the largest number of people, accounting for 42.9% of this group. Overall, the public in the three cities believed that data security under BD cloud computing accounted for 85.3% of the total survey population; the average group accounted for 10% of the total number of respondents; the group that considered unsafe accounted for 4.7% of the total number of respondents. Among the people who believed in data security, they believed that cloud computing BD could better protect data security and provide a secure channel for data transmission. It could also provide timely data encryption and privacy protection to strengthen data security control. The dissatisfied masses believed that BD cloud computing technology was not mature enough and research was not thorough enough. Its environment was unstable, which was prone to data leakage.

7. Optimization Strategy and Experimental Evaluation of AI Data Security in BD Cloud Computing Environment

7.1 Optimization Strategy for AI Data Security under BD Cloud Computing

The optimization of AI data security in the BD cloud computing environment can be optimized

from the following aspects.

7.1.1 National Legal Protection

The promulgation of laws and regulations by the state is a basic guarantee for the protection of the legitimate rights and interests of the market and citizens. With the support of laws and regulations, violations of the law and privacy rights can be prosecuted. Currently, computer data protection laws are relatively weak. In order to protect the privacy rights of AI data, relevant regulatory authorities urgently need to accelerate the formulation and improvement of laws. National regulatory agencies should strengthen supervision, and crack down on excessive collection of personal data and privacy rights. It should severely punish organizations and individuals that infringe on personal privacy rights, so as to protect citizens' personal privacy rights, and establish legal authority.

7.1.2 Improvement of Privacy Technology

The first is to strengthen the theoretical and technical basic research on AI data security. With the help of specific public and social funds, production and research in various fields of society should be controlled, and risk occurrence mechanisms and AI data security protection theories should be jointly studied. Through joint learning, data protection and other core AI data security technologies need to be distinguished. The second is to establish and improve an open source AI learning system, thus providing a basic platform for AI research and development, and ensuring data security. Organizations establish and improve AI open source learning frameworks, and improve embedded data security design and technical measures, so as to encourage the development of open source platforms and industry chain ecosystems through market advantages. Vulnerabilities in the BD environment should be carefully analyzed, and targeted data protection technologies should be researched and developed through data sources, data watermarks, authentication research, anonymous data dissemination, and other research results.

7.1.3 Improvement of Data Security Supervision Methods

First, monitoring and punishment of AI data security: According to national laws and regulations, various ministries and departments monitor and verify AI data through various online and offline means to address AI data security risks such as excessive data collection, data distortion and discrimination, and data resource abuse. Use technical means such as monitoring and public surveillance to quickly detect and increase sanctions, thereby responding to serious errors such as AI network attacks and deep forgery; second, the detection and evaluation of AI data security; an AI platform is to be created for data security detection and evaluation. Security detection and evaluation tools have been developed by developing data security detection and evaluation methods and indicator systems for AI products for application and service development. The security and maturity of AI products have been tested and validated, and AI data security risks have been reduced.

7.2 Experimental Evaluation of Optimization Strategies for AI Data Security under BD Cloud Computing

In order to study the effectiveness of AI data security optimization strategies in BD cloud computing, this article also investigated the data processing speed and legal integrity before and after the use of AI data optimization strategies. A total of three regions were investigated, and the specific survey results are shown in Table 2.

Table 2 Data processing speed and legal integrity before and after the use of AI data optimization strategies

	Before using the AI data security optimization strategy		After using the AI data security optimization strategy	
	Data processing speed	Legal soundness	Data processing speed	Legal soundness
Region 1	68.7%	70.1%	76.8%	80.4%
Region 2	70.5%	72.4%	79.4%	81.6%
Region 3	73.4%	70.6%	78.1%	82.3%

In Table 2, the data processing speed and legal integrity of each region after the use of the AI data security optimization strategy were better than before the use of the optimization strategy. Among them, the data processing speed was 7.2% higher than before use, and the legal integrity was 10.4% higher than before use. Through this experimental analysis, it could be seen that the AI data security in the BD cloud computing environment significantly improved. This was also because data under BD cloud computing could be quickly stored, and could be encrypted, transmitted, and processed through dedicated data transmission channels, with significant performance improvements. In addition, the data processing speed after optimizing AI data security also significantly improved.

8. Conclusions

BD cloud computing is an important trend in the current era, which simplifies people's daily lives. However, it also brings many security issues, thus requiring special attention to security technologies and continuous research and optimization to improve data security and ensure that data and information are not damaged. In the modern digital information era, the application of BD has become a trend. Cloud computing provides a large platform for data analysis and processing based on computer applications. In the BD cloud computing environment, there are still many hidden data security risks. However, after optimizing the AI data security strategy, its data processing speed and legal integrity have significantly improved. Therefore, it is necessary to continuously analyze and study data security issues at different times and stages, and determine appropriate security measures, so as to improve data security and enable BD cloud computing to better ensure data security, thereby better serving humanity.

References

[1] Esposito, Christian. "Blockchain: A panacea for healthcare cloud-based data security and privacy?." IEEE Cloud Computing 5.1 (2018): 31-37.

[2] Isaak, Jim, and Mina J. Hanna. "User data privacy: Facebook, Cambridge Analytica, and privacy protection." Computer 51.8 (2018): 56-59.

[3] Abouelmehdi, Karim, Abderrahim Beni-Hessane, and Hayat Khaloufi. "Big healthcare data: preserving security and privacy." Journal of big data 5.1 (2018): 1-18.

[4] Salman, Tara. "Security services using blockchains: A state of the art survey." IEEE Communications Surveys & Tutorials 21.1 (2018): 858-880.

[5] Xiao, Liang. "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?." IEEE Signal Processing Magazine 35.5 (2018): 41-49.

[6] Lu, Yunlong. "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT." IEEE Transactions on Industrial Informatics 16.6 (2019): 4177-4186.

[7] Taylor, Paul J. "A systematic literature review of blockchain cyber security." Digital Communications and Networks 6.2 (2020): 147-156.

[8] Lo'ai, A. Tawalbeh, and Gokay Saldamli. "Reconsidering big data security and privacy in cloud and mobile cloud systems." Journal of King Saud University-Computer and Information Sciences 33.7 (2021): 810-819.

[9] Sharma, Abhishek, and Umesh Kumar Singh. "Modelling of smart risk assessment approach for cloud computing environment using AI & supervised machine learning algorithms." Global Transitions Proceedings 3.1 (2022): 243-250.
[10] Ray, Soumya, Kamta Nath Mishra, and Sandip Dutta. "Big data security issues from the perspective of IoT and cloud computing: A review." Recent Advances in Computer Science and Communications 12.1 (2020): 1-22.
[11] Shakya, Subarana. "An efficient security framework for data migration in a cloud computing environment." Journal of Artificial Intelligence 1.01 (2019): 45-53.
[12] Bai, Xiang. "Advancing COVID-19 diagnosis with privacy-preserving collaboration in artificial intelligence." Nature Machine Intelligence 3.12 (2021): 1081-1089.
[13] Puthal, Deepak. "The blockchain as a decentralized security framework [future directions]." IEEE Consumer Electronics Magazine 7.2 (2018): 18-21.
[14] Bosri, Rabeya. "Integrating blockchain with artificial intelligence for privacy-preserving recommender systems." IEEE Transactions on Network Science and Engineering 8.2 (2020): 1009-1018.
[15] Hesamifard, Ehsan. "Privacy-preserving machine learning as a service." Proc. Priv. Enhancing Technol. 2018.3 (2018): 123-142.