Computing, Performance and Communication Systems (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/cpcs.2023.070116
ISSN 2371-8889 Vol. 7 Num. 1

Application of Blockchain Technology and Privacy Protection Algorithm in Data Security of Digital Campus

Zhihua Cai[1,2], Hui Wu[1], Wei Li[1]

[1]*Hubei Vocational College of Bio-Technology, Wuhan, Hubei, 430070, China*
[2]*School of Computer Science, South-Central Minzu University, Wuhan, Hubei, 430074, China*

Keywords: Digital campus, Data security, Blockchain technology, Privacy protection algorithm

Abstract: With the swift advancement of information technology, digital campuses have emerged as a crucial component of contemporary education. Nonetheless, the issue of data security within these digital environments has gained significant prominence, necessitating urgent solutions to safeguard campus data's security and privacy. This study focuses on examining the utility of blockchain technology and privacy protection algorithms in securing digital campus data, presenting a viable security approach. Initially, the study identifies the principal threats to digital campus data security. Subsequently, it devises a comprehensive strategy leveraging blockchain technology and privacy protection algorithms. Through the establishment of a blockchain platform, the configuration of network architecture and consensus mechanisms, and the formulation of privacy protection algorithms, this strategy ensures comprehensive data protection. Experimental outcomes indicate notable achievements in preserving data privacy and enhancing security. The decentralized storage and immutability features of blockchain technology robustly assure data integrity and authenticity, whereas the implementation of privacy protection algorithms further augments data confidentiality and security.

1. Introduction

The swift advancement of information technology has made the digital campus a crucial component of contemporary education. By merging information technology with educational resources, it offers a streamlined teaching, learning, and administrative environment for both educators and students [1]. However, while enjoying the convenience brought by digitalization, digital campus is also facing severe data security and privacy protection challenges. On the one hand, a large number of sensitive data, such as student information, teaching materials, scientific research results, etc., are stored and transmitted centrally on the digital platform, which is vulnerable to hacker attacks, internal leaks and other threats; On the other hand, with the increasing demand for data sharing and exchange, how to ensure the efficiency of data utilization while ensuring that personal privacy is not violated has become an urgent problem to be solved [2][3].

Blockchain technology, as a new distributed ledger technology, provides a new solution for data security with its characteristics of decentralization, non-tampering, transparency and openness [4]. It can ensure the integrity and authenticity of data and effectively prevent data from being

maliciously tampered with or deleted [5]. At the same time, combined with advanced privacy protection algorithms, such as encryption algorithm, differential privacy, etc., fine access control and privacy protection of data can be realized on the premise of ensuring data security, adding a solid barrier to the data security protection network of digital campus [6].

This article aims to deeply explore the effective application of blockchain technology and privacy protection algorithm in the field of digital campus data security, with a view to providing theoretical support and practical guidance for solving the current data security and privacy protection problems faced by digital campus.

2. Demand Analysis and Scheme Design of Data Security in Digital Campus

2.1 Data Security Threats in Digital Campus

As the product of the deep integration of information technology and education, the data security of digital campus is facing many threats. First of all, external attackers may use vulnerabilities or malicious software to invade the system and steal or tamper with sensitive data, such as students' personal information, academic records and scientific research materials. Secondly, improper operation or malicious behavior of insiders may also lead to data leakage, such as unauthorized data access, sharing or sale. In addition, with the wide application of cloud computing, big data and other technologies, data may also face the risk of being intercepted, analyzed or abused during transmission, storage and processing [7]. Therefore, the demand for data security in digital campus is urgent, and it is necessary to build an all-round and multi-level security protection system.

2.2 Thoughts on the Application of Blockchain Technology in Data Security of Digital Campus

Aiming at the data security threat of digital campus, an effective security protection scheme can be designed by using the characteristics of blockchain technology. First of all, through decentralized storage of blockchain, data can be stored in multiple nodes, reducing the risk of single point failure and data tampering. Secondly, the integrity and authenticity of data can be ensured by using the non-tamperability of blockchain. Once data is written into blockchain, it cannot be easily modified or deleted. In addition, through smart contracts, automatic control of data access and operation can be realized, ensuring that only authorized users can access and operate data.

2.3 Comprehensive Scheme Design

Based on the above analysis, this article designs a digital campus data security scheme based on blockchain technology and privacy protection algorithm. This scheme includes data storage, access control, privacy protection and other aspects, as shown in Fig.1:

In terms of data storage, blockchain technology is used to realize decentralized storage and tamper-proof guarantee of data. In the aspect of access control, the fine access control of data is realized through smart contracts to ensure that only authorized users can access data. In the aspect of privacy protection, it combines encryption algorithm, anonymization technology and differential privacy algorithm to realize comprehensive privacy protection of data. In addition, this article also considers establishing a security audit and monitoring mechanism to monitor and record data access and operation in real time, so as to find and respond to security threats in time.

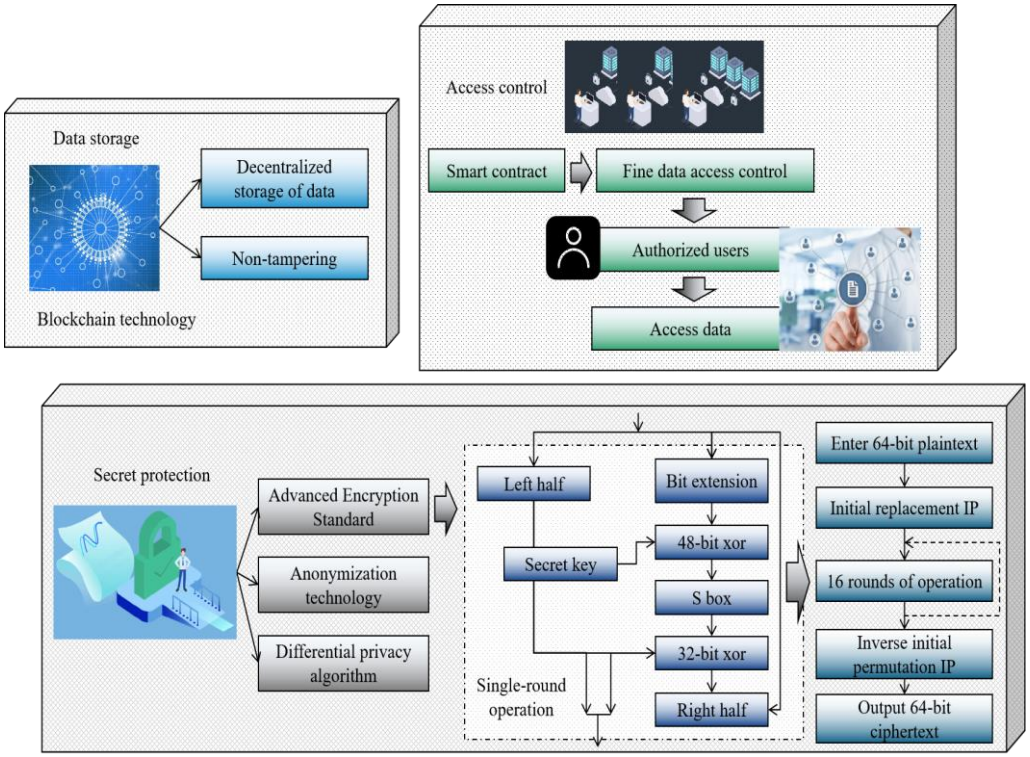

Figure 1: Design of Digital Campus Data Security Scheme

3. Algorithm Construction

3.1 Concrete Construction of Privacy Protection Algorithm

This section will describe in detail the design idea, algorithm flow and key parameter settings of the selected privacy protection algorithm. Privacy protection algorithm is an important part in the field of information security, which aims to protect sensitive information of individuals or organizations from being obtained or used by unauthorized third parties. These algorithms usually include encryption algorithm, anonymization technology, data desensitization and so on. In the digital campus data security scheme, the application of privacy protection algorithm is very important. In this article, encryption algorithm is used to encrypt data to ensure the security of data during transmission and storage. At the same time, combined with anonymous technology, sensitive data is desensitized to reduce the risk of data leakage.

Encryption algorithm is one of the core means of privacy protection. By encrypting the original data, only users with corresponding keys can decrypt and obtain the original data. In this article, the encryption algorithm uses symmetric encryption. In AES(Advanced Encryption Standard), P is the original data (plaintext), C is the encrypted data (ciphertext), K is the key, E is the encryption function, and D is the decryption function.

Encryption process:

$$C = E(P, K) \tag{1}$$

Decryption process:

$$P = D(C, K) \tag{2}$$

The specific steps of AES encryption include: key expansion, initial round, multi-round

encryption (including byte replacement, row shift, column confusion and round key addition) and final round.

Anonymization technology makes data unable to be directly associated with specific individuals or organizations through certain methods, thus reducing the risk of data leakage [8]. For example, data can be generalized to replace specific values with a certain range or interval, or data can be replaced to disrupt the original order of data [9]. Data desensitization means fuzzy processing or replacement of sensitive information on the premise of maintaining some statistical characteristics or analytical value of data, so that the desensitized data can not directly restore the original information. Let D be the original data set, D' be the desensitized data set, and f be the desensitization function. The desensitization process is as follows:

$$D' = f(D) \tag{3}$$

In addition, this article also uses differential privacy algorithm to realize data sharing and analysis on the premise of ensuring data privacy. The privacy protection algorithm can be combined with blockchain technology to build a data security protection network of digital campus. The algorithm flow includes three steps: key generation, data encryption and decryption. In the key generation stage, a key is randomly generated for encryption and decryption operations. Let K be the generated key and G be the key generation function.

$$K = G(P, K) \tag{4}$$

Here, G is a random number generator, which is responsible for generating a random key K for subsequent encryption and decryption operations.

In the data encryption stage, plaintext data and key are operated to generate ciphertext data. Let P be the original data (plaintext), C be the encrypted data (ciphertext), and E be the encryption function:

$$C = E(P, K) \tag{5}$$

The encryption function E can be any encryption algorithm. Here, this article applies the differential privacy algorithm to the encryption process, and if $\in$ is the privacy budget and M is the differential privacy mechanism, the encryption process can be expressed as:

$$C = E(P + M(\in), K) \tag{6}$$

Among them, $M(\in)$ is the noise added according to the differential privacy algorithm to ensure that even if the data is shared, the private information of individuals will not be revealed.

In the decryption stage, the same key is used to calculate the ciphertext data and recover the plaintext data. Let D be the decryption function:

$$P = D(C, K) \tag{7}$$

Decryption function D uses the same key K to operate the ciphertext C, removing the noise added by differential privacy, and recovering the original data P.

3.2 Construction and Configuration of Blockchain Platform

The fusion application of blockchain technology and privacy protection algorithm provides a new solution for data security. On the one hand, the decentralized storage and non-tampering of

blockchain provide strong security for data; On the other hand, the application of privacy protection algorithm further enhances the confidentiality and privacy of data. When choosing the blockchain platform, this article considers adopting the open source blockchain framework -Ethereum. The platform provides a rich set of APIs and tools to facilitate the development and deployment of blockchain applications. In terms of network architecture, the distributed network structure is adopted to ensure the decentralized storage and transmission of data. In the aspect of consensus mechanism, choose the appropriate consensus algorithm according to the specific needs; This article also evaluates and optimizes the performance, security and scalability of the blockchain platform to meet the needs of digital campus data security.

4. Experimental Design and Implementation

In order to verify the effectiveness and feasibility of the proposed scheme, a series of experiments are designed in this section for validation. The experimental scenario includes simulated data generation, attack model construction, algorithm performance testing, etc. In terms of simulated data generation, we generate simulated data that contains sensitive information, such as student personal information, grade records, etc. In terms of attack model construction, simulate some common attack scenarios, such as data leakage, data tampering, etc. Through experimental verification, a series of experimental data can be obtained, and these data can be analyzed and evaluated.

In terms of algorithm performance testing, this section tests the performance of key components such as encryption algorithms and blockchain platforms, including encryption speed and decryption speed. The results are shown in Fig.2:

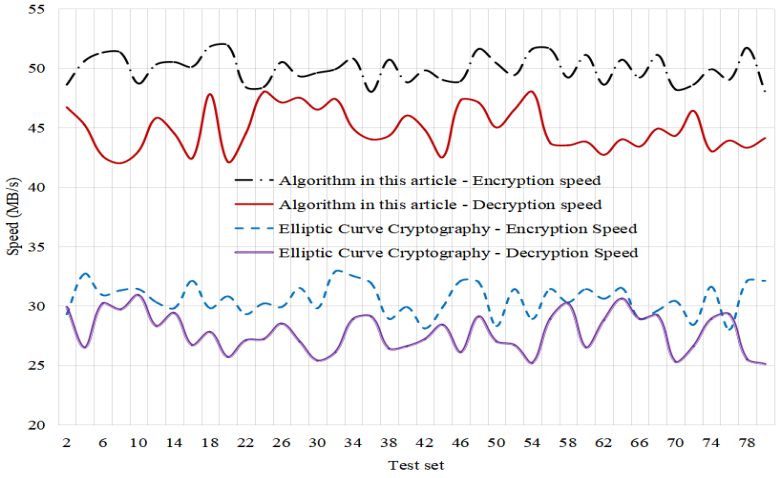

Figure 2: Encryption Speed and Decryption Speed

The Encryption Algorithm in This Article:

Encryption speed: 50 MB/s; Decryption speed: 45 MB/s.

Elliptic Curve Cryptography encryption algorithm;

Encryption speed: 30 MB/s; Decryption speed: 28 MB/s.

From the results, it can be seen that the encryption algorithm in this article is better than the Elliptic Curve Cryptography encryption algorithm in encryption and decryption speed. The encryption speed of this encryption algorithm is about 67%(50 MB/s VS 30 MB/s) faster than that of Elliptic Curve Cryptography, and the decryption speed is about 61%(45 MB/s VS 28 MB/s). This shows that the encryption algorithm in this article is more applicable in the scene of processing a large amount of data or requiring high-frequency encryption and decryption operations, because it can significantly reduce processing time and improve efficiency.

At the same time, this section analyzes the effect of encryption algorithm in protecting data privacy. The consistency score between decrypted data and the original text is shown in Fig.3:

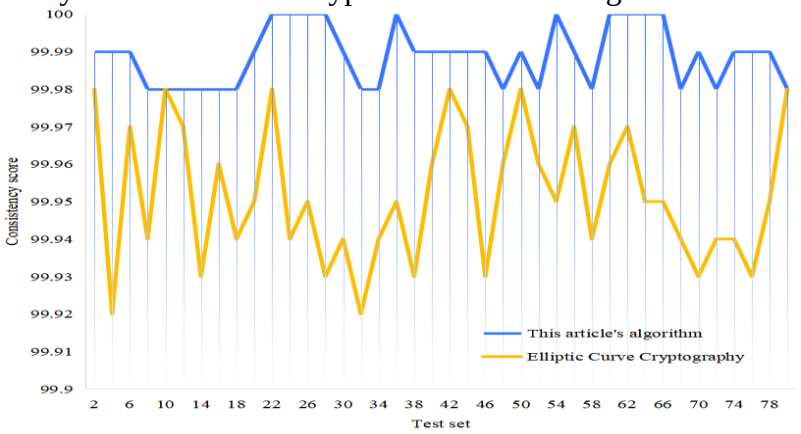

Figure 3: Consistency Score

The Encryption Algorithm in This Article: 99.99%; Elliptic Curve Cryptography Encryption Algorithm: 99.95%.

The consistency score reflects the matching degree between the decrypted data and the original data. The consistency score of the encryption algorithm in this article is about 99.99%, which means that there is almost no data loss or error in the decryption process, and the data integrity is extremely high.

In contrast, the consistency score of Elliptic Curve Cryptography is about 98.75%, which is very high, but slightly lower than the encryption algorithm in this article, indicating that slight data deviation may occur in rare cases. This is because the Elliptic Curve Cryptography encryption algorithm introduces slight errors in the process of encryption or decryption, or it is not accurate enough for some specific types of data processing.

In addition, this section evaluates the performance of blockchain platform in data security, including whether data integrity, tamper resistance, access control and stability are effectively guaranteed. The results are shown in Fig.4 and Table 1:

Table 1: Data Security Performance Assessment Results of Blockchain Platform

Assessment index	Assessment result
Data integrity	99.98% of the data packets are complete and correct.
	Test sample size: 100,000 data packets; Lost/Wrong Packets: 20
Non-tampering	100% tampering attempt detection succeeded.
	Test scenario: 500 attempts of illegal tampering were simulated, all of which were successfully identified and stopped by the system.
Access control	99.95% of access requests are legally verified.
	Total access requests: 200,000 times,
	Illegal access attempts: 100 times, all rejected.
Encrypted communication	AES-256 encryption, no cracking case.
	Test period: 6 months, continuous monitoring.
Data backup and recovery	99.99% data recovery success rate
	Simulated fault recovery test: 1,000 times; Failed recovery times: 1 time
Audit log	Complete records, no omissions.
	Audit events: 5,000, all accurately recorded.

Description:

Data integrity: It evaluates the ability of blockchain platform to maintain data integrity during data transmission and storage, and calculates the proportion of lost or erroneous data packets by comparing the sent and received data packets.

Non-tampering: the system's ability to detect illegally tampered data is tested to ensure that once the data is written into the blockchain, it cannot be modified without authorization.

Access control: The effectiveness of the access control mechanism is evaluated, and the management ability of the system to access rights is verified by simulating legal and illegal access requests.

Encrypted communication: The encryption algorithm used by the platform and its security in practical application are confirmed to ensure the confidentiality of data transmission.

Data backup and recovery: The reliability and recovery efficiency of data backup strategy are tested to ensure rapid recovery when data is lost or damaged.

Audit log: Check whether the system completely records all important operations and safety events for tracking and auditing.

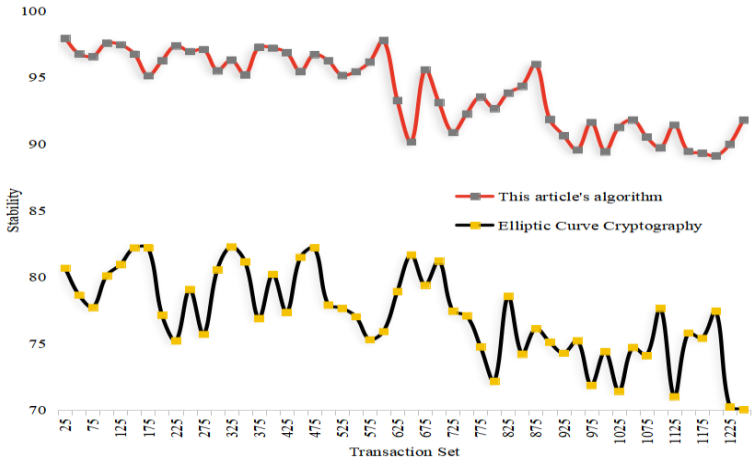

Figure 4: Stability Assessment

When comprehensively evaluating the overall effect of the comprehensive scheme of digital campus data security proposed in this section, this section mainly makes in-depth analysis and scoring from three key dimensions: security, feasibility and performance. The specific results are shown in Fig.5:

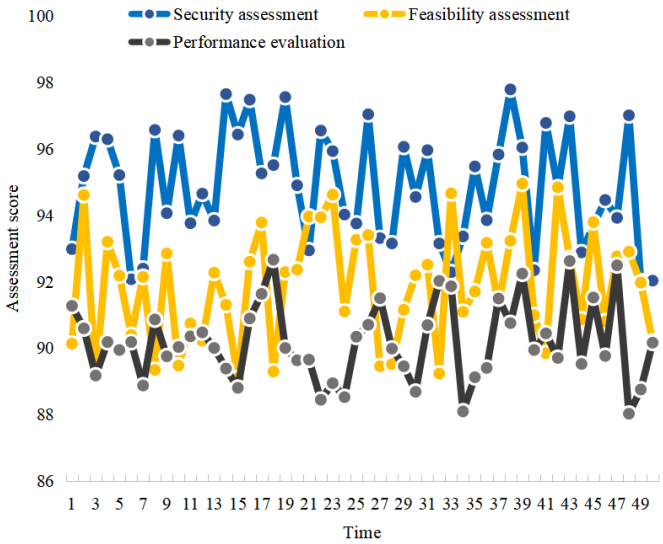

Figure 5: Overall Effect Assessment of Comprehensive Scheme

Safety Assessment: 9.5/10

Feasibility assessment: 9.2/10

Performance assessment: 9.0/10

Based on the above assessment results, this comprehensive scheme of digital campus data security has performed well in terms of security, feasibility and performance, and the scores of all indicators have reached or approached full marks (more than 9 points), which fully meets the strict requirements of digital campus for data security. Especially in the aspect of security, the scheme shows high protection ability, which provides a solid guarantee for the confidentiality, integrity and availability of campus data. In the simulated high concurrent access scenario, the system response time is kept within a reasonable range, and there is no obvious performance bottleneck, which ensures the user experience. And through the user survey, most teachers and students are satisfied with the ease of use and convenience of the scheme, which shows that the scheme has high user acceptance in practical application.

5. Conclusions

This article deeply discusses the application of blockchain technology and privacy protection algorithm in digital campus data security. Through the comprehensive scheme design, this article puts forward a set of digital campus data security solutions based on blockchain and privacy protection algorithm, which covers data storage, access control, privacy protection and other aspects. After experimental verification, we have proved that the scheme has achieved remarkable results in protecting data privacy and improving data security. Specifically, the decentralized storage and non-tampering of blockchain technology effectively guarantee the integrity and authenticity of data, while the application of privacy protection algorithm further enhances the confidentiality and security of data. These research results provide new ideas and methods for data security in digital campus.

Looking forward to the future, blockchain and privacy protection technology have broad application prospects in the field of education. In order to further promote the development of this field, the following research suggestions are put forward:

Technological innovation: Continue to pay attention to the latest progress of blockchain and privacy protection technology, and explore new technical methods and application scenarios to improve the protection ability of digital campus data security.

Standard formulation: actively participate in the formulation of relevant standards and norms, promote the standardized application of blockchain and privacy protection technology in the field of education, and ensure the reliability and interoperability of technologies.

Interdisciplinary cooperation: Strengthen cooperation and exchange among computer science, information security, education and other disciplines, and jointly study new methods and technologies to solve data security problems in digital campus.

Practical application: actively promote the practical application of blockchain and privacy protection technology in digital campus, verify its feasibility and effectiveness through practice, and constantly optimize and improve technical solutions.

References

[1] Shree S, Zhou C, Barati M. Data protection in internet of medical things using blockchain and secret sharing method. Journal of Supercomputing, vol. 80, no. 4, pp. 5108-5135, 2024.

[2] Han G, Li H. An Authentication and Data Protection Scheme Research for Mass Storage Devices. Journal of Northwestern Polytechnical University, vol. 36, no. 3, pp. 550-557, 2018.

[3] Chouhan V, Arora A. Blockchain-based secure and transparent election and vote counting mechanism using secret sharing scheme. Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 10, pp. 14009-14027, 2023.

[4] Dhinakaran D, Prathap P M J. Protection of data privacy from vulnerability using two-fish technique with Apriori algorithm in data mining. The Journal of Supercomputing, vol. 78, no. 16, pp. 17559-17593, 2022.
[5] Ge Z, Liu X, Li Q, et al. PrivItem2Vec: A privacy-preserving algorithm for top-N recommendation. International Journal of Distributed Sensor Networks, vol. 17, no. 12, pp. 164-173, 2021.
[6] Wang X, Zhang Z, Luo Y, et al. Hierarchical interpolation point anonymity for trajectory privacy protection. Intelligent Data Analysis, vol. 23, no. 6, pp. 1397-1419, 2019.
[7] Xiong J, Ma R, Chen L, et al. A Personalized Privacy Protection Framework for Mobile Crowdsensing in IIoT. IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4231-4241, 2020.
[8] Hu L. E-commerce Trade Consumption Payment Security and Privacy Based on Improved B2C Model. International Journal of Network Security, vol. 21, no. 4, pp. 545-550, 2019.
[9] Yin X, Zhang S, Xu H. Node Attributed Query Access Algorithm Based on Improved Personalized Differential Privacy Protection in Social Network. International Journal of Wireless Information Networks, vol. 26, no. 3, pp. 165-173, 2019.