Research Article

Blockchain-Based Encryption Method for Internal and External Health Privacy Data of University Physical Education Class

Zheng Zhou¹ and Yang Liu²

¹Hulunbuir University, Institute of Physical Education, Hulunbuir 021008, Inner Mongolia, China
²Physical Education Institute of Shaanxi Normal University Shanxi, Xi’an 710119, China

Correspondence should be addressed to Yang Liu; liuyang0330@snnu.edu.cn

Received 23 June 2022; Revised 11 July 2022; Accepted 20 July 2022; Published 29 August 2022

Academic Editor: Zhiguo Qu

Copyright © 2022 Zheng Zhou and Yang Liu. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In order to improve the security of the storage and scheduling of health privacy data inside and outside the university physical education class, a storage and scheduling method based on blockchain hybrid encryption is proposed. The distribution structure model of health privacy data blockchain inside and outside the university physical education class is established, arithmetic coding and quantitative feature analysis methods to schedule and adaptively control health privacy data blockchain inside and outside the university physical education class are adopted, public key coding configuration and vector quantization coding methods are combined to design encryption keys in the process of health privacy data transmission inside and outside the university physical education class, and blockchain hybrid encryption algorithm is adopted to design encryption keys for health privacy data inside and outside the university physical education class. The arithmetic coding is embedded in the encryption system, and the bit sequence output by the blockchain hybrid encryption is circularly shifted, so as to realize the encryption of health privacy data inside and outside the university physical education class and optimize the storage scheduling. The simulation results show that this method has good security encryption performance, strong antiattack ability, and balanced storage space allocation, which improves the security storage and transmission ability of health privacy data inside and outside the university physical education class.

1. Introduction

With the rapid increase in network communication data, people pay more attention to storage and scheduling of health privacy data inside and outside physical education classes, but in this process, network attack and virus intrusion will lead to leakage of health privacy data inside and outside physical education class, and the output security is not good. This article constructs a storage and scheduling model of health privacy data inside and outside the physical education class, through coding modulation and key control methods. To realize the storage and scheduling of health privacy data inside and outside the university physical education class, data encryption and arithmetic coding methods are combined and the security storage and information encryption model of health privacy data inside and outside the university physical education class is established [1]. Based on the design of dynamic encryption algorithm of health privacy data inside and outside the university physical education class, combined with dynamic data storage scheme, the security of health privacy data collection inside and outside the university physical education class is improved. The related research on storage and scheduling methods of health privacy data inside and outside the university physical education class has attracted great attention [2].

The storage and scheduling of health privacy data inside and outside the university physical education class is based on the coding and key control of communication encryption data. Nonlinear feature encryption method is adopted to control the storage and scheduling of health privacy data inside and outside the university physical education class.
The traditional methods are mainly BPSK modulation method and chaotic mapping encryption method. Homomorphic mapping encryption method is adopted to control the storage and scheduling of health privacy data inside and outside the university physical education class. In reference [3], a revocable attribute-based encryption algorithm for Internet of Things based on blockchain is proposed, which uses blockchain model analysis and subspace noise reduction reorganization to realize multichannel secure encryption and transmission of health privacy data inside and outside the physical education class. However, this method has poor antiattack ability for multichannel encryption of health privacy data inside and outside the physical education class. In reference [4], a reversible steganography scheme of video encryption domain based on vector histogram migration is designed, and the encrypted transmission of video information is realized through histogram reconstruction, but this method has a large amount of computation and poor stability. To solve the above problems, this article proposes a storage and scheduling method of health privacy data inside and outside the university physical education class based on blockchain hybrid encryption. First, the distribution structure model of health privacy data blockchain inside and outside the university physical education class is established, and the blockchain scheduling and adaptive control of health privacy data inside and outside the university physical education class is carried out by arithmetic coding and quantitative feature analysis. The encryption key design in the process of health privacy data transmission inside and outside the university physical education class is combined with public key coding configuration and vector quantization coding method. Finally, the simulation test shows the superior performance of this method in improving the storage and scheduling ability of health privacy data inside and outside the university physical education class.

2. Multichannel Model and Data Characteristics
Analysis of Health Privacy Data inside and outside Universities in Physical Education Class

2.1. Multichannel Model of Health Privacy Data inside and outside the University Physical Education Class. In recent years, the research on the current situation of college students’ physical exercise has been fruitful, such as the current situation of physical exercise; the relationship between physical exercise and mental health; physical health, social health, and physique; and the research on college students’ attitude, motivation, and habit of physical exercise.

In order to realize the storage and scheduling of health privacy data inside and outside the university physical education class based on blockchain hybrid encryption, first, a multichannel model of health privacy data inside and outside the university physical education class is constructed and the channel output carrier sequence of health privacy data inside and outside the university physical education class is analyzed by using channel equalization method. Channel equalization is an antifading measure taken to improve the transmission performance of communication systems in fading channels. It is mainly to eliminate or weaken the problem of intersymbol interference (ISI) caused by multipath delay in broadband communication. Combined with nonlinear dynamics and statistical physics theory [5], under the background of noise interference, filtering suppression method is adopted.

Digital filter can be divided into two parts: classical filter and modern filter. Classical filter assumes that the useful component and the desired component in the input signal \( x(n) \) are located in different frequency bands, so we can filter the noise through a linear system. If the spectrum of the noise and the signal are mixed, classical filter cannot meet the filtering requirements. There are usually high-pass filter, low-pass filter, band-pass filter, and band-stop filter. Modern filters estimate useful signals and noise signals from noisy signals. In this method, both signal and noise are regarded as random signals, and the signal estimation algorithm is derived by using its statistical characteristics, such as autocorrelation function, cross-correlation function, self-power spectrum, and cross power spectrum, which is then implemented by digital equipment. There are mainly Wiener filter, Kalman filter, and adaptive filter, along with other digital filters.

Classical filtering is an engineering concept based on Fourier analysis and transform. According to the theory of advanced mathematics, any signal that meets certain conditions can be regarded as the superposition of infinite sine waves. In other words, the engineering signal is a linear superposition of sine waves of different frequencies. Sine waves of different frequencies that make up the signal are called frequency components or harmonic components of the signal. In fact, any electronic system has its own bandwidth (the limit on the maximum frequency of the signal), and the frequency characteristic reflects the basic characteristic of the electronic system. The filter is an engineering application circuit designed according to the influence of circuit parameters on the circuit bandwidth. The modern filtering idea is quite different from the classical filtering idea. Modern filtering takes advantage of the randomness of the signal, regards the signal and its noise as random signals, and estimates the signal itself by using its statistical characteristics. Once the signal is estimated, the signal itself is much higher than the original signal-to-noise ratio. Typical digital filters include Kalman filter, Wenner filter, adaptive filter, wavelet transform, and other means. In essence, digital filtering is actually an algorithm that can be implemented on digital devices. These digital devices include not only computers, but also embedded devices such as DSP, FPGA, and arm. Digital filtering has the advantages of high precision, high reliability, programmable change of characteristics or multiplexing, easy integration, and so on. Digital filtering has been widely used in language signal processing, image signal processing, medical biological signal processing, and other application fields. Digital filtering includes low pass, high pass, band pass, band stop, and all pass. It can be time invariant or time-varying, causal or noncausal, linear or nonlinear. The most widely used is linear, time-invariant digital filter. The cepstrum eigenvalues
of the health privacy data output inside and outside the university physical education class contain a subset of features, assuming that \((i, j)\) is the correlation statistical eigenvalue of the health privacy data channel balance control inside and outside the university physical education class, which is the correlation degree between multiple orthogonal subchannels defining the orientation constraint eigenvalues of the main lobe of the array pattern. The process of array mode is shown in Figure 1.

The distribution set of coding links between the array suppression grating lobe and the signal bandwidth is obtained as \(\text{Co}(r)\). Under the condition of blockchain hybrid encryption, based on digital beam forming grating lobe, the spatial sampling frequency parameter \(KC \in \{0, 1, \ldots, n - 1\}\) after digital beam forming grating lobe is obtained, and the broadband true delay energy pattern is constructed in the achievable rate domain \(S_n = \{(j, i, k)\}\). The broadband true delay energy construction process is shown in Figure 2.

The shift number of the signal received by the nth array element, with the minimum number of bits being \(\lceil \log_2(n) \rceil\) bits, establishes the distribution structure model of the health privacy data blockchain inside and outside the university physical education class, and the normal characteristic quantity of the broadband signal incident on the array element is obtained as \(\text{Co}(r)\) [6, 7]. Under optimal position and speed of channel transmission, by using symmetric coding and nonlinear encryption methods, the parameters of the side-grid suppression structure model of the kth cycle are obtained as \(e_k^i = e_k^j\). The three-dimensional spatial scattering cluster is satisfied [8–10]. Based on the modeling of visible area of scattering cluster, the coding and decoding structure block diagram of health privacy data coding inside and outside the university physical education class is obtained by using logistics mapping coding and piecewise linear chaotic mapping method, as shown in Figure 3.

2.2. Analysis of Data Structure Characteristics. Arithmetic coding is used as it is one of the main algorithms of image compression. It is not only a lossless data compression

---

**Figure 1:** Array direction flowchart.

**Figure 2:** Broadband delay construction flow chart.
method, but also an entropy coding method. Other entropy coding methods usually divide the input message into symbols and then encode each symbol, while arithmetic coding directly encodes the entire input message into a number, a decimal $n$ satisfying $0.0 \leq n < 1.0$, and uses quantitative feature analysis. According to the China Securities Association, quantitative trading refers to a trading method that uses a rigorous and complex mathematical or statistical model, with the help of computer, and through the analysis of a large number of historical data, selects an investment method with excess return on probability, and executes it directly by computer. Quantitative trading has a strong objectivity at the transaction execution level, but in essence, its strategic thinking, investment logic, market selection, and even when to start and stop the operation of the computer are all preselected by investors, which make it a highly subjective trading method. The blockchain scheduling and adaptive control of health privacy data inside and outside the university physical education class are carried out [11]. Combined with public key coding configuration and vector quantization coding, the scattering cluster sequence of health privacy data inside and outside the university physical education class is obtained as $X = x_1, x_2, \ldots, x_n$. Turbo code is used to encode and modulate, and the retransmission key of health privacy data inside and outside the university physical education class is expressed as $\bullet \text{RkeyGen}(\text{param}, \text{rskID}, \text{ID}_i, \text{ID}_j)$. Combined with nonlinear balanced scheduling, the block feature matching set $S_n = x_1 + x_2 + \cdots + x_n$ is obtained [12]. The logarithmic function of this encryption interval of health privacy data inside and outside the university physical education class is as follows:

$$I_i = f^{-1}(x)(I_i^{i+1})$$
$$\text{size}(I_i) = P_i \text{size}(I_i^{i+1}),$$

where $I_i^{i+1}$ is the mutual information and $f(x)$ is the state objective function of scattering cluster $N$ after the mth scattering. Assuming that the N-dimensional message vector generated by the source $S$ is represented by $x = (x_1, x_2, \ldots, x_n)$, based on the fitness function $x_i = 2x_i - 1$ analysis of Q cycles, the spatial dynamic matching function

---

**Figure 3**: Block diagram of coding and decoding structure of health privacy data coding inside and outside the university physical education class. (a) Coding process of health privacy data inside and outside universities in physical education class. (b) Decoding process of health privacy data inside and outside the university physical education class.
of health privacy data coding inside and outside the university physical education class is obtained by using random coding modulation:

$$\text{size}(I') = \prod_{n=1}^{M} P(s_i \in S) = \prod_{n=1}^{N} (P_n)^{\text{card}\{s_i | s_i < S_n\}} = \prod_{n=1}^{N} (P_n)^{P_n^M},$$

where $S$ is the broadband true delay energy signal, $s_i$ is the homomorphic key, $P_n$ is the geometric information entropy, and $M$ is the encrypted unstructured characteristic value and it is encrypted as bit sequence. Using the data encryption retransmission mechanism shown in Figure 4, the structural reorganization model of health privacy data inside and outside the university physical education class is established [13].

According to the combined control model of encryption and retransmission structure of health privacy data inside and outside the university physical education class shown in Figure 2, linear grouping is carried out according to the coded data [n, k] [14–16]. In PSK source coding, the coded generator $\psi(x) = v_0 + v_1x + v_2x^2 + \cdots + v_{n-k}x^{n-k}$ of mixed encryption of the blockchain of health privacy data inside and outside the university physical education class is obtained. Under the combined coded re-signing mode, the following results are obtained:

$$-\log_2(\text{size}(I')) = - \sum_{n=1}^{N} P_n^M \log_2(P_n) = M \cdot H,$$

where $I'$ is the data encryption bit rate, $P_n$ is the public key protocol authorized by the key, $M$ is the private parameter, and $H$ is the dynamic characteristic value of the public key. According to the above analysis of the structural characteristics of the health privacy data inside and outside the university physical education class, the encryption key in the process of health privacy data transmission inside and outside the university physical education class is designed by detecting the frequency of compressed coding symbols, combining the public key coding configuration and vector quantization coding method [17]. The discrete key transmission sequence of health privacy data inside and outside the university physical education class is constructed by using the natural mode expansion sequence of chaotic logistics, and the feature decomposition model of health privacy data storage inside and outside the university physical education class is established by using the method of random linear feature detection, as shown in Figure 5.

3. Optimizing the Storage and Scheduling of Health Privacy Data inside and outside the University Physical Education Class

3.1. Blockchain Hybrid Encryption Algorithm. In view of the security threat of quantum computing to blockchain ciphers and the long-term security challenge to blockchain systems, the design theory of blockchain cipher algorithms with anti-quantum computing capability is studied, and blockchain cipher algorithms such as data encryption and digital signature that can resist quantum attacks are designed. Blockchain cryptographic protocols such as identity authentication, secure communication, and secure consensus that can resist quantum attacks are designed. The anti-quantum security
blockchain system design theory and data security storage technology are researched and the anti-quantum security blockchain prototype system design method proposed, followed by researching on the fast and secure implementation technology of anti-quantum security public key cryptosystem and studying the solution for migration from the existing cryptographic technology to the anti-quantum computing cryptographic technology in the blockchain.

The blockchain hybrid encryption algorithm is used to design the encryption key of health privacy data inside and outside the university physical education class. In the process of cyclic code displacement [18], the bilinear mapping of data encryption is given as: \( x_{ib} = x_{ib} - \delta_{ib} \) (1 \( \leq i \leq \beta \)). The private key of blockchain hybrid encryption is: \( \delta_{ib} = [x_{ib}]_p + \xi_{ib} \cdot \pi - CRT_{\rho_{mn}}(2r_{ib,\mu n}1)_{m, n \in \mathbb{N}}^{\rho} \cdot r_{ib,\mu n} \rightarrow \mathbb{Z} \cap (-2^{\rho-1}, 2^{\rho-1}) \), \( \xi_{ib} \rightarrow \mathbb{Z} \cap [0, 2^{\rho \log_2(\rho) + \rho} - \eta] / \pi \).

In the complete set of attributes of blockchain hybrid encryption key, a retransmission scheme is given. The generation algorithm of user key is described as \( x'_{ib} = x_{ib} - \delta_{ib} (1 \leq i \leq \mu) \), and the throughput rate of encryption scheme is \( \delta_{ib}' = [x'_{ib}]_p + \xi'_{ib} \cdot \pi - CRT_{\rho_{mn}}(2r'_{ib,\mu n}1)_{m, n \in \mathbb{N}}^{\rho} \cdot r'_{ib,\mu n} \rightarrow \mathbb{Z} \cap (-2^{\rho-1}, 2^{\rho-1}) \). The encrypted data is shared to the private key through the public channel, and the identification bit is: \( \xi'_{ib} \rightarrow \mathbb{Z} \cap [0, 2^{\rho \log_2(\rho) + \rho} - \eta] / \pi \).

Based on the error correction redundancy logout method, the security parameters of the input key are given as follows: \( \Pi_{ib} = x_{ib} - \delta_{ib} (1 \leq i \leq \mu) \), where \( \delta_{ib} = (x_{ib})_p + \xi_{ib} \cdot \pi - CRT_{\rho_{mn}}(2r_{ib,\mu n}1)_{m, n \in \mathbb{N}}^{\rho} \cdot r_{ib,\mu n} \). The output ciphertext protocol is: \( \omega_{ib,\mu n} \rightarrow \mathbb{Z} \cap (-2^{\rho-1}, 2^{\rho-1}) \), \( \xi_{ib,\mu n} \rightarrow \mathbb{Z} \cap [0, 2^{\rho \log_2(\rho) + \rho} - \eta] / \pi \).

The user is made to convert the public key of the key: \( pk^* = (x_0, s, \epsilon_1, (\delta_{ib})_{1 \leq i \leq \beta, 0 \leq b \leq 1}, (\delta_{ib})_{1 \leq i \leq \mu, 0 \leq b \leq 1}, (\delta_{ib})_{1 \leq i \leq \beta, b \mu \leq 1}, (\delta_{ib})_{1 \leq i \leq \mu, b \mu \leq 1})) \), according to the corresponding private parameter \( x_{ib}, x'_{ib}, \Pi_{ib} \), by optimizing the construction of sparse set; the private key protocol of edge data is: \( sk^* = (p_{ib})_{1 \leq i \leq \beta} \).

To encrypt \((pk, m_{ij}) \in \mathbb{Z}^{\rho \times \rho}\), the security parameter characteristics of Turbo code are analyzed, and the encryption key obtained is: \( b = (b_{ij})_{1 \leq i \leq \beta} \in (-2^{\rho}, 2^{\rho} \rho \rho \beta) \) and \( b = (b'_{ij})_{1 \leq i \leq \beta} \in (-2^{\rho}, 2^{\rho} \rho \rho \beta) \); the source coding feature quantity is recovered to obtain the output ciphertext: \( c^* = \sum_{1 \leq i \leq \beta} m_{ij} \cdot x_{i,0, j} + \sum_{1 \leq i \leq \beta} b_{ij} \cdot \Pi_{i,0} \cdot \Pi_{i,1} + \sum_{1 \leq i \leq \beta} b_{ij} \cdot x_{i,0, j} \cdot x_{i,1, j} \).

To decrypt \((sk, c^*, z)\), cyclic code displacement parameters are output to obtain information source parameters: \( m = (m_{ij}) \), where \( m_{ij} = c^* / p_{ij} \), 1 \( \leq i, j \leq \mu \).

With encrypted retransmission, bit rate of data points is: \( x_{i,0, j} \mod p_{ij} = 2r_{i,0, j} + \delta_{i,0, j} \) + add \((pk, c^*, c^*)\). Bus transmission data parameters are: \( c^* \mod x_{0, j} \).

With encryption algorithm, \((pk, m_{ij}) \in \mathbb{Z}^{\rho \times \rho}\) is encrypted. The generated ciphertext is \( c \), the symbol frequency detection output characteristic quantity is: \( c^* \mod x_{0, j} \), and the encrypted data becomes: \( c \mod p_{ij} = c^* / (c_1, \mod p_{ij}, \ldots, c, \mod p_{ij}) \). Introducing blockchain hybrid encryption technology, the coding structure of stop and wait encrypted output is shown in Figure 6.

According to the above analysis, the blockchain hybrid encryption algorithm is used to design the encryption key of the health privacy data inside and outside the university physical education class, and the arithmetic code is embedded in the encryption system to design the multichannel secure transmission [19–22].

3.2. Multichannel Secure Transmission of Data. A method for transmitting data such as audio/video (AV) data over multiple channels includes selecting data and encrypting information, and encrypting the information with the encrypted information to generate encrypted data. The encrypted information is divided into several parts. The encrypted data is transmitted using at least one of the plurality of channels, and at least some portions of the encrypted information are transmitted on at least one channel other than the channel on which the encrypted data is transmitted. More generally, the encrypted data is transmitted on one channel, and the encrypted information is divided and transmitted on several other channels.

The encryption sparse expression method is introduced to establish a dynamic detection factor analysis model of health privacy data transmission inside and outside the university physical education class. The inverse function of \( f(x) \) is used to store the scheduling value, and coupling vectors of health privacy data inside and outside the university physical education class is: \( b = (b_{ij})_{1 \leq i \leq \beta} \in (-2^{\rho}, 2^{\rho} \rho \rho \beta) \) and \( b = (b'_{ij})_{1 \leq i \leq \beta} \in (-2^{\rho}, 2^{\rho} \rho \rho \beta) \) satisfy

\[
c = b \times \sum_{1 \leq i \leq \beta} b_{ij} \cdot x_{i,0, j} \cdot x_{i,1, j}.
\]

According to the chaotic coding scheme of logistics [23], a multichannel output model of network data is established. The multichannel transmission feature sequence is: \( s = [s_i, i = 1 \ldots M | s_i \in \mathcal{S}] \); key parameters are

\[
P_n = 1/M \cdot \text{card}[s_i | s_i = S_n].
\]

Among them, \( S_n \) represents the transmission ratio between channels, \( M \) represents the key sequence block, and a complete ciphertext sequence is obtained. Thus, multichannel secure transmission is achieved through blockchain hybrid encryption [24].
Based on key inquiry, the output key forgery feature quantity is SD. Based on the above analysis, the bit sequence output by blockchain hybrid encryption is circularly shifted to realize the storage and scheduling of health and privacy data inside and outside the university physical education class. The implementation process is shown in Figure 7 [25].

As shown in Figure 7, the storage and scheduling process of health privacy data inside and outside college physical education classes mainly starts with formulating a homomorphic public key encryption mechanism, designing an encryption key, and then designing a decryption key according to the length of the output data packet. On this basis, the characteristic distribution of encrypted bit sequence is determined, the symbol frequency is detected according to the distribution results, the key is filled, and the optimization of data encryption is realized, so as to complete the storage and scheduling of health privacy data inside and outside college physical education classes and also the research on the encryption method of health privacy data inside and outside college physical education classes based on blockchain.

4. Simulation Experiment

In order to test the performance of this method in realizing the storage and scheduling of health and privacy data inside and outside the university physical education class, a simulation experiment was conducted. The calculation theory for the full life cycle protection of privacy information selects the health privacy data inside and outside college physical education classes as the test object, uses MATLAB simulation to get the information before and after storage scheduling, compares it, and determines the effectiveness of the method against statistical attacks through information distribution. Under normal circumstances, if the information is evenly distributed and flat, it is judged that the proposed method has good antistatistical characteristics; and if on the contrary, the proposed method has poor antistatistical characteristics. The network data sample length is 1200, the data transmission time interval is 0.37 s, the bandwidth is 45 kHz, and the parameters of multichannel transmission are shown in Table 1.

The number of layers of health privacy inside and outside the university of physical education class is set as follows: the confidence of data encryption is 0.869, and the circular displacement of health privacy data inside and outside the university of physical education class is 5.48. See Table 2 for the feature distribution of encrypted data.

According to the parameter settings in Tables 1 and 2, the encrypted storage design of health privacy data inside and outside the university physical education class is carried out [26]. The channel dynamic characteristic parameters are selected to obtain health privacy data inside and outside the university physical education class, as shown in Figure 8.

It can be seen from Figure 8 that for three different encrypted data samples, the time domain waveform distribution of health privacy data inside and outside college physical education classes is relatively uniform, with good results. Taking the time domain waveform data of health privacy data inside and outside college physical education classes in Figure 8 as the test object, under the test environment, through MATLAB simulation, the data security encrypted transmission output of the proposed method is calculated and the encrypted output results obtained, as shown in Figure 9.

By analyzing Figure 9, we can see that the recessive ability of using this method to encrypt health privacy data inside and outside college physical education classes is good, the level of scrambling is high, and the three different encrypted data samples show a good state. The antiattack ability of this method, reference [4] method, and reference [5] method is tested. The encryption performance is shown in Table 3.

According to the comparison results in Table 3, compared with the methods in reference [4] and reference [5], the recognition degree of this method is as high as 97.62%, and the time cost is only 0.43 s. Its antiattack ability is good, the encryption performance is good, and the recognition ability and secure transmission ability of data are improved. The reason is that in the process of multichannel secure transmission of data, the method in this article uses at least one of the multiple channels to transmit the encrypted data.

---

Figure 7: Implementation process of encryption of health privacy data inside and outside the university physical education class.
Figure 8: Time domain waveform of health privacy data inside and outside the university physical education class. (a) Encrypted data sample 1. (b) Encrypted data sample 2. (c) Encrypted data sample 3.
and transmits the encrypted data on one channel, and the encrypted information is divided and transmitted on several other channels, which is conducive to enhancing the performance of the method in this article.

To sum up, the encryption method of health privacy data inside and outside college physical education classes based on blockchain has good recessive ability, high scrambling level, strong antiattack ability, and good encryption performance.

5. Conclusions

Through coding modulation and key control methods, the storage and scheduling of health privacy data inside and outside college physical education classes are realized. This article proposes a storage and scheduling method of health privacy data inside and outside college physical education classes based on blockchain hybrid encryption. The following conclusions are obtained through the study:

1. The time domain waveform distribution of health privacy data inside and outside college physical education classes is relatively uniform
2. This method has better implicit ability and higher scrambling level in storing and scheduling health privacy data inside and outside college physical education classes

| Method                        | Leakage probability | Deciphering bit length (Kbit) | Recognition degree (%) | Time expenditure (s) |
|-------------------------------|---------------------|--------------------------------|------------------------|----------------------|
| Methods of this article       | 0.056               | 1.21                           | 97.62                  | 0.43                 |
| Reference [4]                 | 0.085               | 9.56                           | 86.34                  | 0.65                 |
| Reference [5]                 | 0.093               | 12.48                          | 91.55                  | 1.79                 |

Figure 9: Data encryption output. (a) Encrypted data sample 1. (b) Encrypted data sample 2. (c) Encrypted data sample 3.
This method has good security and strong antiattack ability in storing and scheduling health privacy data inside and outside college physical education classes.

Data Availability

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding this work.

Acknowledgments

This work was supported by Research on Teaching Reform of Higher Education in Jilin University of Architecture and Technology, “Application and Practice of Flipped Classroom in Physical Education” (JY2021C006).

References

[1] Z. Yin, Z. Yang, and C. Li, “Study on integration of health data in and out of university physical education courses based on ‘Internet plus’,” *Journal of South China Normal University (Social Science Edition)*, vol. 45, no. 4, pp. 108–114, 2020.

[2] L. I. Bai, “Study on the correlation of PE courses and students’ physical health in colleges,” *Sport Science and Technology*, vol. 41, no. 3, pp. 160–164, 2020.

[3] J. Wang and C. Zhang, “Remote data encryption storage method based on blockchain technology,” *Journal of Hebei North University (Natural Science Edition)*, vol. 37, no. 11, pp. 19–25, 2021.

[4] Z. Li, H. Zhang, L. Wang, and X. Feng, “Encryption of stereo image based on fractional chaotic system and RNA encoding,” *Journal of Taiyuan University of Technology*, vol. 52, no. 5, pp. 718–727, 2021.

[5] D. Wang, “Research on network data sharing technology based on blockchain and privacy protection,” *Journal of Henan Institute of Science and Technology (Natural Sciences Edition)*, vol. 48, no. 3, pp. 74–78, 2020.

[6] J. Su and X. Chen, “The platform architecture, application prospect and actual challenges of blockchain for students fitness test,” *Journal of Nanjing Institute of Physical Education*, vol. 34, no. 1, pp. 21–26, 2020.

[7] W. Guan, “Design of network privacy data security protection model based on block chain,” *Journal of Langfang Teachers University (Natural Science Edition)*, vol. 21, no. 4, pp. 29–33, 2021.

[8] X. Xiang and S. Shi, “Structural innovation of multi-centre collaborative governance for Students’ physical health based on blockchain technology,” *Hebei Sports Science*, vol. 40, no. 9, pp. 762–765, 2021.

[9] Z. Jianming, Z. Qinnan, G. Sheng, D. Qingyang, and Y. Liping, “Privacy preserving and trustworthy federated learning model based on blockchain,” *Chinese Journal of Computers*, vol. 44, no. 12, pp. 2464–2484, 2021.

[10] X. Liang, J. Wu, Y. Zhao, and K.-T. Yin, “Review of blockchain data security management and privacy protection technology research,” *Journal of Zhejiang University*, vol. 56, no. 1, pp. 1–15, 2022.

[11] M. Hongwei, T. Cong, L. Jun, Z. Dangang, and S. Wenlue, “Research on data sharing and exchange method based on blockchain,” *Journal of the Hebei Academy of Sciences*, vol. 38, no. 1, pp. 17–23, 2021.

[12] Z. Zheng, “Cluster analysis of students’ physique health data based on self-organizing feature mapping network method,” *Sichuan Sports Science*, vol. 39, no. 3, pp. 53–56, 2020.

[13] L. Liu, “Research on the mode of college physical education curriculum under the background of quality standard,” *Journal of Jilin Agricultural Science and Technology College*, vol. 31, no. 1, pp. 117–119, 2022.

[14] H. Fu, “Study on the behavior intention of college students’ physical exercise based on structural equation model,” *Bulletin of Sport Science & Technology*, vol. 29, no. 7, pp. 119–121, 2021.

[15] R. Wang, C. Zhong, and L. I. Guiying, “An empirical study on key competences of innovative and entrepreneurial talents in sports industry based on SEM,” *Journal of Shandong Institute of Commerce and Technology*, vol. 21, no. 5, pp. 84–90, 2021.

[16] R. Guo, “Research on network data privacy protection method based on blockchain technology,” *Modern Information Technology*, vol. 4, no. 13, pp. 164–166, 2020.

[17] G. Chang, “Design of security encryption system for network link transport layer key database,” *Modern Electronics Technique*, vol. 43, no. 15, pp. 74–77, 2020.

[18] Z. Tan and C. Tang, “A survey on privacy protection techniques in blockchain system,” *Journal of Guangzhou University*, vol. 20, no. 4, pp. 1–15, 2021.

[19] Z. Xiaodong, C. Taowei, Y. Yimin, and W. Huiyuan, “Access control scheme based on blockchain and CPABE,” *Application Research of Computers*, vol. 39, no. 4, pp. 986–991, 2022.

[20] Y. J. Wang, C. T. Cao, and Y. O. U. Lin, “A novel personal privacy data protection scheme based on blockchain and attribute-based encryption,” *Journal of Cryptologic Research*, vol. 8, no. 1, pp. 14–27, 2021.

[21] S. Wei, L. Long, W. Wenhao, Zhenghua, and D. Wenhao, “Research on the credible supervision technology of data privacy over blockchain,” *Software Guide*, vol. 20, no. 12, pp. 1–8, 2020.

[22] S. Li, N. Wang, and X. Du, “Privacy protection mechanism of on-demand disclosure on blockchain,” *Chinese Journal of Network and Information Security*, vol. 6, no. 3, pp. 19–29, 2020.

[23] Q. Shi, “Design and optimization of storage scheme for real-time data sharing system of Sports competitions,” *Software Engineering*, vol. 24, no. 3, pp. 48–51, 2021.

[24] X. Zonglian, W. Chongyu, Z. Xiaoming, Z. Yukun, and C. Ruidong, “Searchable encryption scheme based on blockchain and supporting access control,” *Radio and Communications Technology*, vol. 47, no. 3, pp. 269–276, 2021.

[25] W. Zhou, “Breaking through the difficult position of physical education curriculum in colleges and universities under the thinking of Sports powerful country in the new era and the way of breakthrough,” *Sichuan Sports Science*, vol. 39, no. 1, pp. 134–137, 2020.

[26] M. Li, C. Gu, and M. Wen, “Secure charging transaction data storage platform based on blockchain,” *Computer Engineering and Applications*, vol. 56, no. 21, pp. 79–84, 2020.