Hindawi
Journal of Sensors
Volume 2023, Article ID 9812029, 1 page
https://doi.org/10.1155/2023/9812029

Retraction

Retracted: Hybrid Encryption Algorithm for Sensitive Information of College Physical Fitness in Cloud Storage Environment

Journal of Sensors

Received 8 August 2023; Accepted 8 August 2023; Published 9 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] M. Deng, "Hybrid Encryption Algorithm for Sensitive Information of College Physical Fitness in Cloud Storage Environment," *Journal of Sensors*, vol. 2022, Article ID 1552437, 10 pages, 2022.

Hindawi
Journal of Sensors
Volume 2022, Article ID 1552437, 10 pages
https://doi.org/10.1155/2022/1552437

Research Article

Hybrid Encryption Algorithm for Sensitive Information of College Physical Fitness in Cloud Storage Environment

Miaolei Deng

College of Information Science and Engineering, Henan University of Technology, Zhengzhou 450001, China

Correspondence should be addressed to Miaolei Deng; dengmiaolei@haut.edu.cn

Received 2 August 2022; Accepted 23 August 2022; Published 10 September 2022

Academic Editor: Yaxiang Fan

In order to improve the security of college sports fitness sensitive information, this paper proposes a hybrid encryption algorithm for college sports fitness sensitive information in cloud storage environment. Build an analysis model of influencing factors of cloud storage environment to identify the risk value of sensitive information; Using Bloom filter data structure to eliminate redundant data of sensitive information; The transmission channel model of sensitive information and the security coding model of sensitive information are constructed. Combined with the fuzzy differential information fusion method, the complete key of sensitive information under the symmetric encryption protocol is obtained to realize the key optimization design. Through AES encryption and decryption algorithm, the anti encryption control and structural reorganization of college sports fitness sensitive information, and the iterative convergence control of hybrid encryption, so as to realize the hybrid encryption of college sports fitness sensitive information. The encryption time of the design algorithm under different attribute numbers is always kept below 0.2S, the maximum encryption time under different number of software packages is only 0.5 s, and the encryption accuracy can reach 1, which proves that the design algorithm has certain application value.

1. Introduction

With the development of sports fitness in Colleges and universities, the security of sports fitness data transmission has attracted more and more attention [1]. It is very important to establish an optimized control model for the transmission of physique sensitive information in Colleges and universities, and adopt optimized encryption algorithm to improve the encryption ability of physique sensitive information [2, 3]. Based on this, some scholars have studied it, For example, Wang l et al. [4] introduced a new IND-CCA secure multi instance framework for code based hybrid encryption primitives in random oracle model. This method is based on the direct construction of key generation function and one-way trapdoor function. The input is labeled to achieve more strict security loss and smaller private key size. F Hasan [5] proposed an algorithm based on hybrid supervised regression classification learning. The algorithm adopts the hybrid structure of classifier and regression learner to realize data encryption. The results show that the algorithm is faster than the original problem and has less computing resources. Z Yu Lei et al. [6] proposed a sensitive information encryption scheme based on format retention in the identity password environment. Compared with the existing format retention encryption scheme, the communication parties do not need to transfer the key, and generate the encryption key and decryption key through the key derivation function. The security of sensitive information transmission is improved by using hybrid encryption. It is proved that the scheme meets the security of identity based pseudo-random permutation and has the indistinguishability of ciphertext under adaptive selective plaintext attack. L Xiao Feng et al. [7] proposed an intelligent encryption algorithm for medical sensitive information based on quantum computing. Firstly, the key construction of quantum encryption of medical sensitive information is designed by considering the mixed entangled state, and the protocol subspace matrix constructed in the key is analyzed to form the key information Then, by calculating the neighborhood distribution function of information, the separation matrix quantum coding is constructed to provide processing data for key rearrangement. Considering the interference of quantum entangled states and their additional states, effective key encryption is carried out, and finally the intelligent encryption of medical sensitive information is realized. The experimental results show that this method has good anti attack ability, high transmission efficiency and good overall performance. Although the above methods have realized the encryption of sensitive information or data, the algorithm is very complex and the security performance is low, so it is not suitable for the encryption of sensitive information of physical fitness in Colleges and universities with large amount of data.In order to solve the above problems, this paper proposes a hybrid encryption algorithm for college sports fitness sensitive information in cloud storage environment.

2. Preprocessing Sensitive Information of College Physical Fitness under Cloud Storage Environment

2.1. Identification of Sensitive Information of Physical Fitness in Colleges and Universities. There are many groups of data with different attributes and different sources in the cloud storage environment, which may become factors affecting the security of sensitive information. When these factors change suddenly, the sensitive information in college physical fitness does not have protective measures, so there are great management risks in the whole college physical fitness. When users pay attention to privacy, there are two measurement dimensions of information risk: severity and susceptibility. Combined with the sensitive information protection and management standard [8], the influencing factor analysis model shown in Figure 1 is constructed.

Use the model shown in Figure 1 to identify the risk categories of college sports fitness sensitive information in the cloud storage environment. First, identify the management risk, which is the risk problem caused by poor information management in the overall service process [9]. When such a situation occurs, the cloud storage server has monitoring interruption or server crash [10]. Secondly, identify technical risks. In the process of cloud storage service, due to the interception of malicious software, the server is attacked, the entire monitoring environment becomes extremely fragile, and the sensitive information of files exposed in the air is stolen by other clients. Finally, identify the risk of information disclosure. The confidentiality level of sports fitness information in some colleges and universities is high, which may store extremely important political, economic and cultural information. When the server is attacked, the leakage of such information will annoy many management departments and regions. Based on the above analysis, there are three main risk categories of sensitive information. The influencing factor analysis model constructed this time sets the information judgment data layer according to the above risk categories in advance, and uses the calculation process of the following formula to identify whether there are risks in sensitive information and identify the degree of risk. The formula is:

$$\begin{cases} \mathrm{F_i} = \sum_{\mathrm{i}}^{\mathrm{n}} \lambda_{\mathrm{i}} \\ \mathrm{R} = \int_{\mathrm{F_i}}^{\mathrm{Q}} (\mathrm{F_i}, \mathrm{H_{t+1}} | \mathrm{H_t}) \, \mathrm{dF_i} \end{cases} \quad (1)$$

Where $\mathrm{F_i}$ represents the risk identification result; λ_{i} represents i different influencing factors obtained by the model; R represents value at risk; $\mathrm{H_t}$ and$\mathrm{H_{t+1}}$ represents the running state of cloud storage environment at time t and time t +1, respectively. According to the above formula, the influencing factor analysis model determines and identifies the category and risk degree of sensitive information, so as to provide reliable data for the setting of encryption level.

2.2. Eliminate Sensitive Information and Redundant Data. There is a large amount of redundant data in the physical sensitive information of colleges and universities, which affects the encryption speed of sensitive information [11]. Therefore, it is very important to eliminate redundant data in sensitive information before encryption. Bloom filter can be used to retrieve whether an element is in a set, so as to eliminate the data that does not belong to the set. Its advantage is that the spatial efficiency and query time are much better than general algorithms. Therefore, the process uses data structure bloom filter to reduce the file characteristics of sensitive information. It is known that the structure is obtained by mapping and compression of multiple hash functions, represents an independent data set by vector U, and judges whether the factors obtained by the influencing factor analysis model belong to this set. This structure uses m hash functions to calculate. These functions are $\mathrm{h_i}, \mathrm{h_2}, \cdots, \mathrm{h_m}$, respectively. While calculating all hash function values [12], set the array value of the corresponding n-bit length to 1. When using Bloom filter structure to search redundant data, use the same hash function to obtain m hash results. When there is a value not 1 in the m bit of the corresponding n-bit array, it can be determined that the data sequence does not belong to the rule set. When the results are all 0, the misjudgment rate p is used to determine that the data sequence belongs to the rule set. According to the above assumptions, the bloom filter data structure is constructed. The specific process is as follows:

Set the number of bits to k, and the initial value of all bits of the bloom filter data structure should be 0; Select two hash functions and record them as $\mathrm{h_1}$ and $\mathrm{h_2}$, respectively, to perform the data mapping task; Use two sets of functions to calculate the summary value under each identifier, and set the bit position of the data structure to 1; Output the result of Bloom filter as the characteristic value of sensitive information file. According to the above steps, determine the number of common 1 of these sensitive information files in bloom filter according to the similarity index of the two files. Referring to the calculation method of cosine similarity [13],

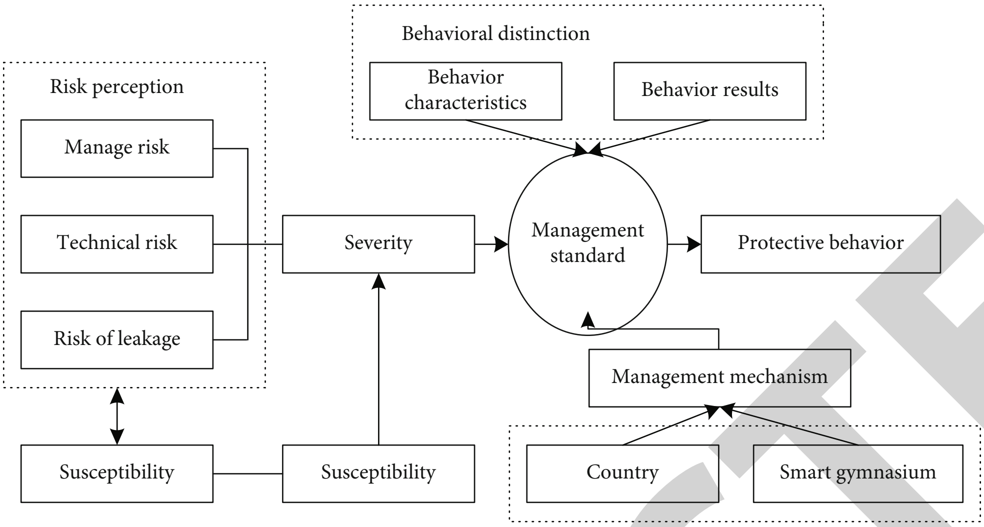


Figure 1: Analysis model of influencing factors of cloud storage environment.

the document similarity index is obtained, and the calculation formula is:

$$\mathrm{Sim}(u, v) = \frac{\sum_{i=1}^{n} u_i v_i}{\sqrt{\sum_{i=1}^{n} u_i^2 \sum_{i=1}^{n} v_i^2}} \tag{2}$$

Where u and v represent different sports fitness information sensitivity documents. When m hash functions map all elements to different arrays, the probability that a bit in these arrays is still 0 can be calculated by the following formula:

$$\dot{r} = \left(1 - \frac{1}{n}\right)^{ms} \tag{3}$$

Where 1/n represents a bit probability of a random hash function; $(1 - 1/n)$ indicates the probability that this bit is not recognized after one calculation. Therefore, in order to realize all data mapping, perform ms-th hash calculation to obtain:

$$\lim_{n \longrightarrow +\infty} \left(1 - \frac{1}{n}\right)^{-n} = \mu^{ms} \tag{4}$$

If the proportion of 0 in the array is γ, the error rate is calculated as follows:

$$(1 - \gamma)^m \approx (1 - r)^m \tag{5}$$

Where $(1 - \gamma)$ represents the proportion of digit group 1; $(1 - \gamma)^m$ represents the area where 1 is just recognized, so the value of misjudgment rate p is obtained:

$$p = \left(1 - \mu^{-(ms/n)}\right)^m \tag{6}$$

Using the above calculation process, the redundant data in the sensitive information file is determined and eliminated, which provides a prerequisite for fast encryption.

2.3. Mixed Encryption of Sports Fitness Sensitive Information

2.3.1. Sports Fitness Sensitive Information Coding. In order to realize the hybrid encryption of sensitive information about physical fitness in Colleges and universities in the cloud storage environment, first, build a key protocol for the encryption of sensitive information about physical fitness in Colleges and universities. Combined with the arithmetic coding method and key design [14], establish a link layer transmission protocol for sensitive information about physical fitness in Colleges and universities. Since the wheel code is the first practical and feasible code that can approach the Shannon limit, it has superior performance under the condition of low signal-to-noise ratio, And it can be applied in many fields. Therefore, this paper uses turbo coding as the coding sequence [15], and combines the methods of key recombination and packet forwarding to obtain the transmission channel model of university sports fitness sensitive information, as shown in Figure 2.

In the transmission channel structure model of sports fitness sensitive information in Colleges and universities shown in Figure 2, the chaotic modulation method [16] is used to obtain the encrypted sensitive transmission coding sequence. Through the fuzzy chaotic key control method, the delay D_{t+1} and captain sequence L_{t+1} of mixed encryption of sports fitness sensitive information at t+1 time are solved, and the expression is as follows:

$$\begin{aligned} D_{t+1} &= \delta_{t+1}(1 - \lambda)^2 \int_{t+1}^{t} f(t + 1)dt \\ L_{t+1} &= \lambda(t + 1) + \delta_{t+1} \int_{t+1}^{t} f(t) + f(t + 1)dt \end{aligned} \tag{7}$$

Where δ_{t+1} is the sensitive coding sequence in the sensitive information transmission channel structure.

In the process of user key generation, analyze the symmetric key of college sports fitness sensitive information. Through the method of output key encapsulation, the input

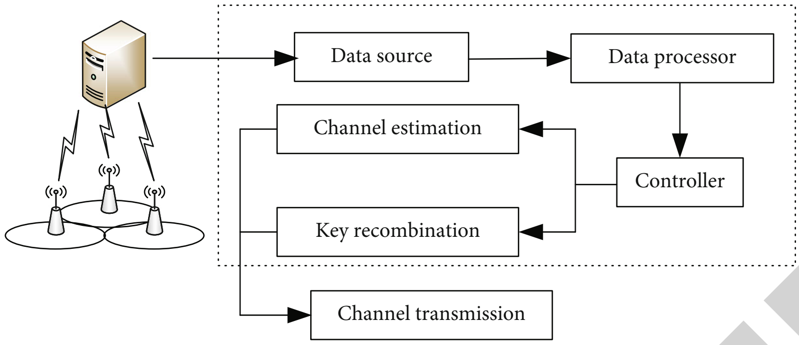


Figure 2: Transmission channel model of sensitive information of physical fitness in Colleges and Universities.

Table 1: Simulation test environment.

Name	Explain
Virtual machine	VM10.0
Processor	AMD A4-4300M 2.5GHz ×1
Memory	3GiB
Graphical	AMD
Hard disk	50GB
Operating system	Ubuntu 15.04 64bits
Kernel version	3.19.0-15-generic
Search engine toolkit	Lucene2.4.3

security parameters are as follows:

$$A = \lambda\sqrt{D_{t+1} - \frac{L_{t+1}}{\delta_{t+1}(t)}} \tag{8}$$

Define the length of the sensitive information of physical fitness in Colleges and universities to be encrypted as N, construct the sensitive characteristic quantity of physical fitness in Colleges and universities by using the symmetric hash function [17], use the distribution of 0 and 1 to carry out the error correction control of physical fitness encryption in Colleges and Universities, and obtain the transmission protocol of sensitive key of physical fitness in Colleges and universities according to the input system parameters:

$$\begin{gathered} C \longrightarrow S : \text{Certificate } A \\ C \longrightarrow S : \text{Exchange } D_{t+1} - N \\ C \longrightarrow S : \text{Verify } L_{t+1} + N \end{gathered} \tag{9}$$

Using the method of symbol frequency feature decomposition, the security coding model of college sports fitness sensitive information is obtained as follows:

$$T_{\text{service}} = \sqrt{\lambda A} + \frac{\varepsilon_S + \lambda_S}{\rho} \tag{10}$$

Where ε_S is the characteristic component of cloud storage, λ_S is the covariance function [18], and ρ is the symbol frequency of college sports fitness sensitive information.

After obtaining the security coding model of sports fitness sensitive information in Colleges and universities, the key design of sports fitness sensitive information is realized by using the method of public key replacement.

2.3.2. Key Design of Sports Fitness Sensitive Information. Firstly, the method of replacing identity is used to mark the physical fitness key linearly, and the parameter information entropy of college physical fitness sensitive information is $H_2(x)$. The method of role distribution convergence key control is used to decrypt the private key, and the convergence key ciphertext is:

$$K = \frac{[\beta_2(x) + \alpha_2(x)]^2}{H_2(x)} \tag{11}$$

Where $\beta_2(x)$ represents the encryption symmetry function of sensitive information of physical fitness in Colleges and universities, and $\alpha_2(x)$ represents the Gaussian distribution function satisfying variance α. Using the method of convergent key control, a new transmission sequence $X = x_1, x_2, \cdots, x_n$ of college sports fitness sensitive information is constructed, and the binomial of sequence X is counted. It is obtained that the normal distribution characteristic quantity of college sports fitness sensitive information meets:

$$F = k(w) + \frac{X}{\theta} \tag{12}$$

Where k(w) is the probability density function of non overlapping block matching; θ distributes the convergence key for the role.

Using the method of differential fusion analysis, the identification bit of college sports fitness sensitive information data block is obtained, which is expressed as:

$$X_i = FK\sqrt{D_{t+1} - \frac{{L_{t+1}}^{w}}{\delta_{t+1}(t)}} \tag{13}$$

Where w is the amount of recoverable data files.

Based on the identification bit of the sensitive information data block and combined with the fuzzy differential information fusion method, the complete key of college

Table 2: Sharing performance parameters of different sensitive information encryption methods.

Sharing scheme	Test group a	Test group b	Test group c	Test group d
Attribute hiding	√	—	—	—
Property undo	√	—	—	√
User revocation	√	√	√	√
Computing outsourcing	√	—	—	√
Fine grained access	√	√	√	√
Sharing mode	Many to many	One to many	One to many	One to many

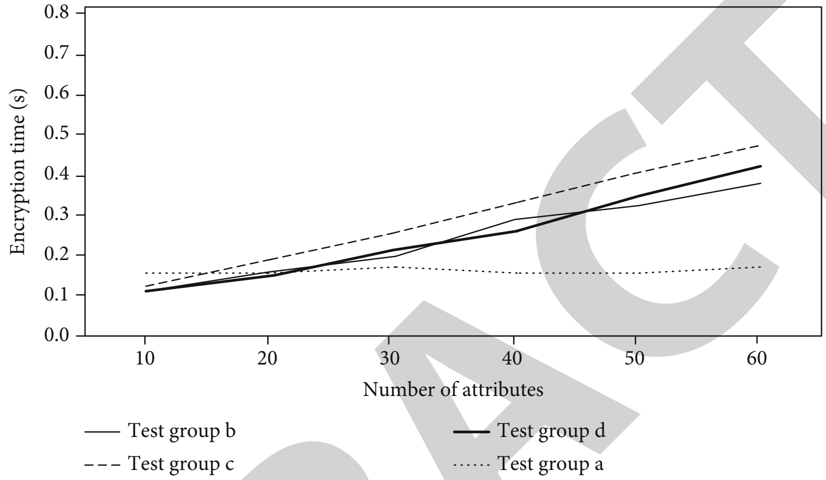


Figure 3: Encryption time under different attribute numbers.

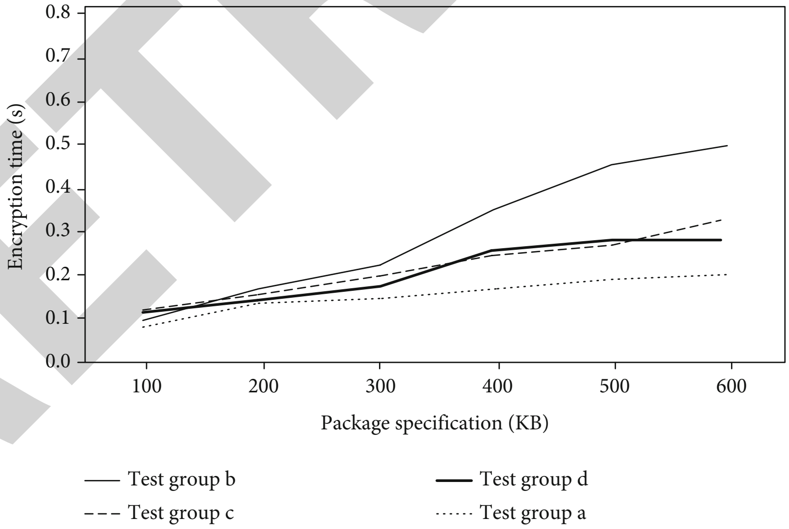


Figure 4: Encryption time under different package specifications.

sports fitness sensitive information under the symmetric encryption protocol is obtained, which is expressed as:

$$\sigma = \mathrm{Sim}(\mathrm{u}, \mathrm{v})\mathrm{T}_{\mathrm{service}} + (\mathrm{X}_{\mathrm{i}} + 1)^2 \tag{14}$$

Observe the mixed encryption strength and complete the key design of sports fitness sensitive information, so as to improve the ability of data encryption transmission and privacy protection.

2.4. Optimization of Mixed Encryption of Sports Fitness Sensitive Information

2.4.1. AES Encryption and Decryption Algorithm. In the process of AES(Advanced Encryption Standard) encryption, the

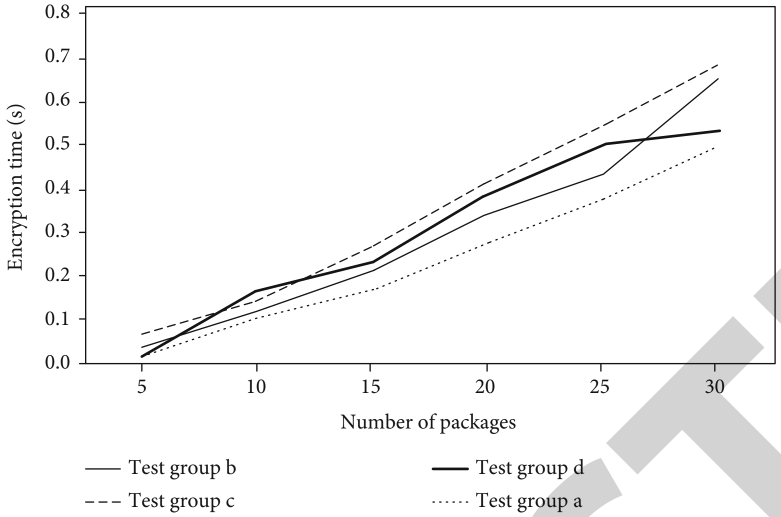


Figure 5: Encryption time under different number of packages.

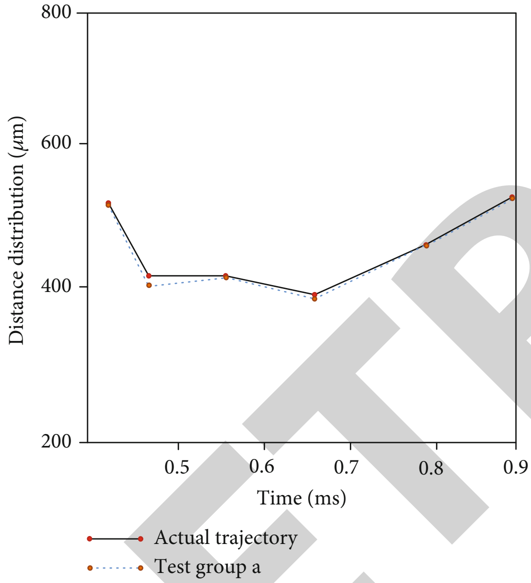


Figure 6: Data encryption output trace line.

statistical characteristic P is obtained by performing the frequency detection in the block. The key protocol of linear encryption is obtained by using the methods of chaotic homomorphic mapping [19] and elliptic linear encryption, which is expressed as:

$$G(x) = \sigma_{\text{service}} + PX_i \tag{15}$$

Thus, it is obtained that the output discrete statistical characteristic quantity of the encryption of college sports fitness sensitive information is described as:

$$C = \Delta H + F\int_{X=1}^{N} G(X)dx \tag{16}$$

When the length of the bit sequence is n and the block length is m, after obtaining the corresponding block length parameters, the random probability characteristic distribution of college sports fitness sensitive information encryption is obtained as follows:

$$V = C\int_{i=1}^{n} \frac{1}{\Delta H}\sum_{i=1}^{n} u_i v_i di \tag{17}$$

Under the key protocol of linear encryption, the statistical characteristics of frequency detection in the block are obtained. According to arithmetic coding and chaotic key control, the AES encryption algorithm for the statistical characteristics of sports fitness sensitive information is as follows:

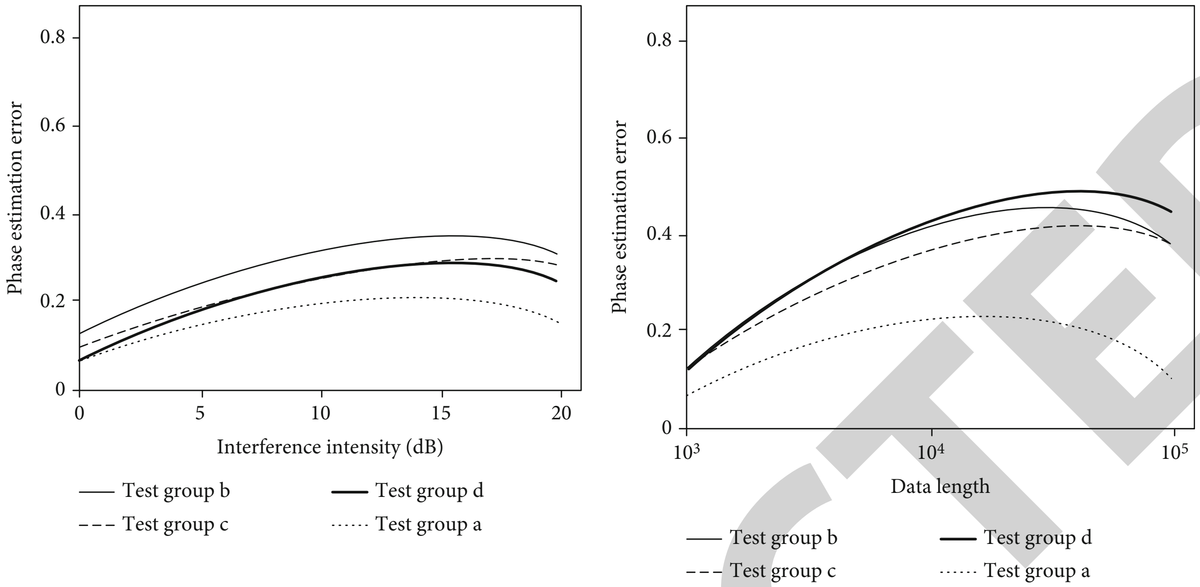
$$W_{\text{service}} = G(x)\sqrt{\frac{V}{2}} \tag{18}$$

Assuming that the chaotic encrypted copy of the heterogeneous cryptosystem is J, under the adaptive ciphertext attack, the decryption algorithm of sports fitness sensitive information is as follows:

$$Y = A(W_{\text{service}} + \sigma_{\text{service}})^2 \tag{19}$$

According to the above calculation results, the optimization design of AES encryption and decryption algorithm is realized.

2.4.2. Mixed Encryption of Sports Fitness Sensitive Information. Through AES encryption method [20], the anti encryption control and structural reorganization of college sports fitness sensitive information are carried out, and the measurement information of college sports fitness sensitive



(a) Different interference intensity

(b) Different data length

Figure 7: Comparison of estimation errors of sensitive information.

Table 3: Comparison of detection and recognition accuracy (%).

Number of experiments	Test group a	Test group b	Test group c	Test group d
20	0.923	0.823	0.575	0.765
40	0.989	0.856	0.789	0.794
60	1.000	0.894	0.896	0.817
80	1.000	0.894	0.918	0.852

information meets the following requirements:

$$r_{imax} = \frac{n + Y}{2^{imax+2}} \tag{20}$$

Where imax is the longest convergent key ciphertext.

In the longest frequency detection model, the frequency of imax and AES encryption is r_{imax}. assuming that the private key of the data block and the identification component of the data block are represented by M, the hybrid encryption iterative function of university sports fitness sensitive information encryption is obtained as follows:

$$Z = \text{sum}(imax) + \frac{\sqrt{r_{imax}}}{N} \tag{21}$$

Combined with the hybrid encryption iteration, the detection statistics shall meet the following convergence control form:

$$\varphi = Z - 2n\pi(1 - \pi) \tag{22}$$

Under the optimized encryption block length, the statistical characteristic quantity of linear encryption key is obtained, which is expressed by ω and obeys the standard normal distribution function. Finally, the data ciphertext and convergence key are sent to the encryption key, and the mixed encryption model of sports fitness sensitive information is obtained as follows:

$$E = \frac{1}{\omega} \sum_{n=1}^{N} \left[Z + \frac{n\pi(1 - \pi)}{Y} \right] \tag{23}$$

This paper realizes the hybrid encryption of sports fitness sensitive information, and completes the design of sports fitness sensitive hybrid encryption algorithm in Colleges and universities by using AES encryption and decryption algorithm.

2.5. Simulation Test Analysis. In order to verify the effectiveness of the proposed hybrid encryption algorithm for college sports fitness sensitive information in cloud storage environment, the simulation test is carried out on MATLAB tool.

2.5.1. Simulation Preparation. The setting of simulation test environment parameters is shown in Table 1.

Assuming that the test environment under the parameters in Table 1 is stable and safe, test the hybrid encryption performance of the proposed method for sensitive information in the process of college sports fitness information sharing. In order to ensure that the experimental test results can fully explain the effectiveness of the data, this method is compared with the existing three groups of encryption methods in reference [5], reference [6] and reference [7], and three groups of comparative encryption methods are set as Test group b, Test group c and Test group d, respectively. The proposed method is Test group a, and Table 2 shows the shared performance parameters of the four groups of encryption methods.

In Table 2, attribute hiding means that when the user accesses the shared data, the random attributes not associated with the attribute information are difficult to identify the pairing. Even if the attacker obtains the value, it does not know the data attribute Association, so it has the hiding function. Attribute revocation when users need to revoke attributes, they can use cloud sending to delete the attribute set stored locally. User revocation means that the user needs to revoke and send the data to be deleted by using the private cloud to realize user deletion. Computing outsourcing is the process of sharing data. Private cloud generates ciphertext. Through computing outsourcing, the complexity of the signature algorithm is reduced and the amount of computation is reduced. Fine grained access is to design corresponding restriction conditions for each shared data, and determine the access users through the conditions.

3. Results and Analysis

In order to ensure that the test results are more convincing, the number of 60 access attributes is set in the first stage of the experiment. Figure 3 shows the encryption time test results of four groups of encryption methods under the same test conditions.

According to the test results shown in Figure 3, as the number of attributes increases during the access process, the encryption time of test group B and test group candtest group increases, while there is no obvious correlation between the encryption time of test group A and the number of attributes. Although the number of attributes continues to increase, the encryption time has been in a stable state, always kept below 0.2S, which proves that the encryption efficiency of the design method is higher. The reason for this phenomenon is that the encryption process of the four groups of encryption methods is different. Compared with the three encryption methods, the calculation is more complex, so it takes longer time. In the second stage of the experiment, different file packages are set. Figure 4 shows the encryption time test results under different file package specifications.

According to the test results shown in Figure 4, when the file package specifications are different, the encryption time of all methods increases with the increase of the file package volume. Among them, the encryption time of Test group b is the highest, and the encryption time of the other three groups is relatively close, but generally speaking, Test group a of the method in the representative text takes the least time. This is because test B needs to block the data before encryption. Therefore, when the volume of the file package is larger, the more blocks need to be divided and the longer the time will be. In the third stage, set different number of packages. Figure 5 shows the encryption time test results of four groups of methods under different number of packages.

According to the test results shown in Figure 5, the encryption time of the four groups of methods increases rapidly with the increase of the number of packets. However, compared with the other three groups, the encryption time of the test group is the shortest, and the maximum is only 0.5 s, which is far lower than the encryption time required by the other three methods. Therefore, it is proved that under the conditions of the third test stage, the encryption method proposed in this paper is slightly better than the other three groups of encryption methods.

The length of sensitive information of physical fitness in Colleges and universities is 1600 μm. The length of the block is 200 points μm. The packet size is 120 μm. The transmission delay of sports fitness sensitive information is 0.67 ms, and the size of data file is 12GB. The distribution of data encryption track line is shown in Figure 6.

According to the analysis of Figure 6, the output stability of the sensitive information encryption of college sports fitness by this method is high, which is basically consistent with the encryption track, and can improve the encryption ability of sensitive information.

Test the phase estimation error of sports fitness sensitive information under different data interference intensity and different data length. In order to enhance the statistical convenience of the experimental results, set the error unit as unit 1, and the results are shown in Figure 7.

When the error of the three groups of interference (a) is 2.0, it is known that the error of the four groups of interference (a) in the simulation method increases by 2.0. Compared with the four groups of interference, when the error of the three groups of interference (a) is the largest in the test process. The experimental results in Figure 7(b) show that when the data length increases, the sensitive information recognition errors of the three methods are quite different. In contrast, the application of test group a was least affected by the data length. The above experimental results show that the identification error of sensitive information in test group a is low, and the application stability is strong.

In order to further verify the application accuracy of Test group a, test the accurate recognition rate of different methods under fixed interference intensity and data length. The number of experimental iterations is 80 times, and the accuracy unit is 1. The specific output data results are shown in Table 3.

Analysis of Table 3 shows that when the interference intensity and data length are the same, the recognition accuracy of Test group b also improves with the increase of the number of experimental iterations, but the highest accuracy is 0.894, which can not meet the requirements of encryption of sensitive information of physical fitness in Colleges and universities. When the number of experiments reaches 80, the recognition accuracy of Test group c reaches 0.918, but when the number of experiments is small, the accuracy of this method is 0.5 ~ 0.8, indicating that the application of this method is not stable enough and the recognition accuracy fluctuates greatly. The test accuracy of group D fluctuated between 0.76 and 0.86, which was relatively stable, but the accuracy was still lower than that of group A. The accuracy of Test group a is high. When the number of experiments reaches more than 60, the recognition accuracy of Test group a reaches the highest value, which shows that under the support of the number of experiments, the method achieves the best stability and application performance.

4. Conclusions

In order to improve the security of college sports fitness data transmission, this paper proposes a hybrid encryption algorithm for college sports fitness sensitive information in cloud storage environment. Using turbo code as the coding sequence, combined with the methods of key reorganization and packet forwarding, the transmission channel model of college sports fitness sensitive information is obtained. According to the mixed encryption strength and combined with the fuzzy differential information fusion method, the representation of college sports fitness sensitive key and the transmission protocol of college sports fitness are constructed to realize the mixed encryption of college sports fitness sensitive information encryption and secret stealing. The encryption time of the design algorithm under different attribute numbers is always kept below 0.2S, the maximum encryption time under different number of software packages is only 0.5 s, and the encryption accuracy can reach 1, which proves that the design algorithm has certain application value. Based on the above research, it can be proved that the algorithm designed in this paper has a good application and development prospect in the field of sensitive information encryption of physical fitness in Colleges and universities, and is also of great significance to sensitive information encryption in other fields. However, the algorithm did not analyze the encryption effect of sensitive data in other fields during the experiment. Therefore, if you want to extend it to more fields, you need further experimental analysis to optimize the shortcomings of the algorithm and realize its application in many fields.

Data Availability

The dataset can be accessed upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work received Research and Practice Project of Higher Education reform in Henan Province (2019SJGLX083): Research and practice of teaching quality monitoring system and guarantee mechanism based on OBE concept.

References

[1] A. García-Hermoso, I. Hormazábal-Aguayo, O. Fernández-Vergara et al., “Physical fitness components in relation to attention capacity in Latin American youth with overweight and obesity,” *Scandinavian Journal of Medicine and Science in Sports*, vol. 30, no. 7, pp. 1188–1193, 2020.

[2] S. G. Liang and Z. Tao, “Research on Attribute Encryption Simulation of Distributed Internet Sensitive Information,” *Computer Simulation*, vol. 38, no. 5, 2021.

[3] Z. Guan, W. Yang, L. Zhu, L. Wu, and R. Wang, “Achieving adaptively secure data access control with privacy protection for lightweight IoT devices,” *Science China Information Sciences*, vol. 64, no. 6, pp. 1–14, 2021.

[4] L. Wang, J. Chen, K. Zhang, and H. Qian, “A post-quantum hybrid encryption based on QC-LDPC codes in the multiuser setting,” *Theoretical Computer Science*, vol. 835, no. 4, pp. 82–96, 2020.

[5] F. Hasan, A. Kargarian, and J. Mohammadi, “Hybrid Learning Aided Inactive Constraints Filtering Algorithm to Enhance AC OPF Solution Time,” *IEEE Transactions on Industry Applications*, vol. 57, no. 2, pp. 1325–1334, 2021.

[6] Z. Y. Lei, L. G. Ping, and Z. Y. Jie, “A format preserving encryption scheme for sensitive information,” *Computer Engineering and Science*, vol. 42, no. 2, pp. 236–240, 2020.

[7] L. X. Feng, J. H. Shuang, and W. Y. Wei, “Intelligent encryption algorithm of medical sensitive information based on quantum computing,” *Journal of Jilin University(Information Science Edition)*, vol. 38, no. 6, pp. 694–701, 2020.

[8] J. K. MirtschM and K. Blind, “Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis,” *IEEE Transactions on Engineering Management*, vol. 68, no. 1, pp. 87–100, 2021.

[9] V. E. Okeke, C. Nwakoby, and N. E. Okeke, “Excessive internal borrowings and debt management: implications on the Nigerian economy,” *Journal of Financial Risk Management*, vol. 11, no. 1, pp. 116–141, 2022.

[10] F. Chen, F. Meng, T. Xiang, H. Dai, J. Li, and J. Qin, “Towards usable cloud storage auditing,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 31, no. 11, pp. 2605–2617, 2020.

[11] H. Yuan, X. Chen, J. Wang, J. Yuan, H. Yan, and W. Susilo, “Blockchain-based public auditing and secure deduplication with fair arbitration,” *Information Sciences*, vol. 541, no. 9, pp. 409–425, 2020.

[12] V. P. Gaikwad, J. V. Tembhurne, C. Meshram, and C. C. Lee, “Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function,” *The Journal of Supercomputing*, vol. 77, no. 8, pp. 8281–8304, 2021.

[13] S. Guo, L. Ren, Y. Xu et al., “Dimension reduction calculation method of toroidal magnet,” *IEEE Transactions on Applied Superconductivity*, vol. 30, no. 4, pp. 1–6, 2020.

[14] M. Johnson, S. Kishore, and D. M. Berwick, “Medicare for all: an analysis of key policy issues,” *Health Affairs*, vol. 39, no. 1, pp. 133–141, 2020.

[15] A. J. G. BaleviE, “Autoencoder-Based error correction coding for one-bit quantization,” *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3440–3451, 2020.

[16] A. Ouannas, A. Karouma, G. Grassi, V. T. Pham, and V. S. Luong, “A novel secure communications scheme based on chaotic modulation, recursive encryption and chaotic masking,” *Alexandria Engineering Journal*, vol. 60, no. 1, pp. 1873–1884, 2021.

[17] S. Ramos-Calderer, E. Bellini, J. I. Latorre, M. Manzano, and V. Mateu, “Quantum search for scaled hash function preimages,” *Quantum Information Processing*, vol. 20, no. 5, pp. 1–28, 2021.

[18] X. Ma and M. B. Blaschko, “Additive tree-structured conditional parameter spaces in Bayesian optimization: a novel covariance function and a fast implementation,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 43, no. 9, pp. 3024–3036, 2021.

[19] L. Meng, S. Yin, C. Zhao, H. Li, and Y. Sun, “An improved image encryption algorithm based on chaotic mapping and discrete wavelet transform domain,” *International Journal of Network Security*, vol. 22, no. 1, pp. 155–160, 2020.

[20] A. F.-X. Ametepe, A. S. R. M. Ahouandjinou, and E. C. Ezin, “Robust encryption method based on AES-CBC using elliptic curves Diffie–Hellman to secure data in wireless sensor networks,” *Wireless Networks*, vol. 28, no. 3, pp. 991–1001, 2022.