# HIGH-DENSITY INFORMATION SECURE STORAGE METHOD FOR BIG DATA CENTER BASED ON FUZZY CLUSTERING

**Zili Chen**
*Fujian Chuanzheng Communications College, Fuzhou, 350007, China*
*E-mail: fjjyczl@163.com*

***ABSTRACT**: High-density information security storage in big data center is the important application of ensuring the confidentiality of information. Information storage security is mainly for the high-density information in big data center of the network. A security storage method of high-density information in big data center based on fuzzy clustering is proposed. In order to improve the accuracy of high-density information security storage in big data centers, the fuzzy theory is firstly used to give the distribution structure of high-density information, and obtain the time series flow model of information security storage and the time interval of high-density data distribution. Experimental simulation shows that the data storage security and stability of the proposed method are high, it is of great significance for the security of network information. The simulation experiment results show that with the increase of the sampling time, the throughput of using the proposed method for high-density information security storage in the big data center has obvious advantages compared to that of the method , it greatly enhances the quality of high-density information security storage in the big data center.*

***KEYWORDS**: Big data center; High-density information; Security storage*

## 1 INTRODUCTION

In China, with the advent of the Internet era, the Internet is used in the construction of various industries. People are increasingly dependent on the computer and data center, information storage security risks are increasing. high-density information security storage in big data center is the important application of ensuring the confidentiality of information. Information storage security is mainly for the high-density information in big data center of the network. Different information data can come from different data sources. For example, there are data from semi-structured data, unstructured data, and so on. This part of the structure can contain a variety of confidential records, so in order to save the data, it must have a large enough capacity of storage space, but also need a good security measures. However, in the process of high-density information storage, the vector quantization feature of the high-density information attribute set in big data center cannot be extracted accurately in the process of high-density information storage relative to most of the information storage methods, leading to the high-density information security storage into a bottleneck. In this case, the problem of high-density information security storage in big data center, has become an important factor restricting the development of big data storage, causing a lot of experts and scholars attention.

In (Kumar, Srivastava.2014), the generalized balanced binary search tree is used to preserve and encode, allowing the user to define the encryption algorithm and the adjustment strategy. Giving the encrypted information preserves the order of the plaintext, to obtain the objective function of high-density information security storage in the big data center, get the constraints of security storage, and complete the security storage of high-density information in big data center. The data storage efficiency of this method is high, but it cannot extract the vector quantization feature of the high-density information attribute set in big data center, and the storage security and stability are poor. In reference (Wu, Wang, Liang, et al. 2016), the correlation coefficient and evenness index are selected to construct the comprehensive objective function of high-density information security storage in big data center. The control parameters of the composite chaotic cryptosystem are used for security storage of high-density information in big data center and coordinate the optimal setting. On this basis, the high-density information security storage in big data center is completed. The method is more reliable, but the storage process is more cumbersome and time-consuming. In (NIU Geng. 2015), the information storage encryption matrix of compressed onion layer and extended onion column is proposed. The plaintext-ciphertext correspondence rule of high-density information is designed, and the mutual conversion between the

name of plaintext column and ciphertext column is given. Based on this, the high-density information security storage in big data center is completed. The method is extensible, but the storage cost is high.

Aiming at the above problems, a security storage method of high-density information in big data center based on fuzzy clustering is proposed. Experimental simulation shows that the data storage security and stability of the proposed method are high, it is of great significance for the security of network information.

## 2 THE OVERALL ARCHITECTURE OF HIGH-DENSITY INFORMATION SECURITY STORAGE IN BIG DATA CENTER

The overall architecture of the security storage platform of high-density information in big data center is divided into four levels, followed by data storage layer, data management layer, data service layer and user access layer. The overall architecture of the storage platform is shown in figure 1.

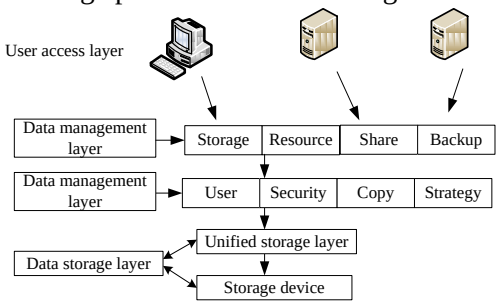


**Fig. 1 The Overall Architecture of High-density Information Security Storage Platform**

The main purpose of the security storage system of high-density information in the big data center is to build a platform for today's facing problems of data security and information processing in big data systems, and provide solutions. The operation flow is: on the client, when the user selects the high-density information that needs to be uploaded, the client program encrypts the high-density information. After that, the encrypted ciphertext is uploaded to the server. The server accepts the ciphertext data sent from the client, and stores the ciphertext data and the corresponding information on the server. When this user and other users with data sharing rights need to use the data, download the ciphertext data from the server, and decrypts it on the client to get its plaintext message; when the user searches the keywords, the client will encrypt the keywords into ciphertext firstly, and then return the ciphertext keywords to the server, after the server receives the keywords, the stored ciphertext data are retrieved.

The security storage system of high-density information in data center is divided into three functional modules, which are defined as follows:

(1) upload / download data module of client. The module not only contains the information transmission between the server and the client, but also contains the upload to the server, the encryption of plaintext and decryption of ciphertext when data is downloaded from the server;

(2) data processing module of server. The module contains the storage of ciphertext uploaded by the user and the storage of its ciphertext sharing information;

(3) The retrieval module that acts on the client and server. On the client, when the user inputs the keywords that they want to retrieve, the client will encrypt the keywords and upload it to the server at the same time, and retrieve the ciphertext.

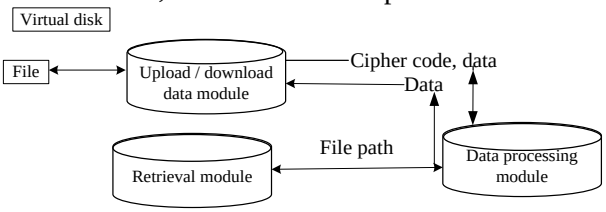


**Fig. 2 Structure of Storage Function Module in the High-density Information Security Storage System**

The high-density information security storage system contains two structural modules, which are defined as follows:

1) client module of high-density information storage. The module can be responsible for high-density information encryption, decryption, ciphertext data upload and download, and the encryption of retrieval keywords.

2) high-density server module. The module mainly contains the ciphertext data and the corresponding information from the client, stores them on the server, and the search process is mainly responsible for the matching of ciphertext retrieval words.

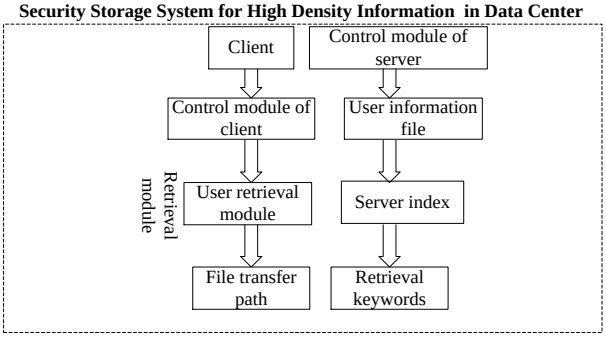


**Fig. 3 Structure of Storage System**

The high-density information security storage system, contains two structural modules, four control modules, shown as follows:

1) Registration module of client. New users will be through the module, added to the high-density information security storage system. The trusted third party, through the user registration information forms a pair of keys for the new user, and distributes to the new user.

2) Login module of client. Users will be connected to the server through this module, on this basis, data upload, download, delete and other operations are carried out.

3) Control module of server. Through the module, the server masters the user's connection, and works together with the control module of server to achieve keywords search function.

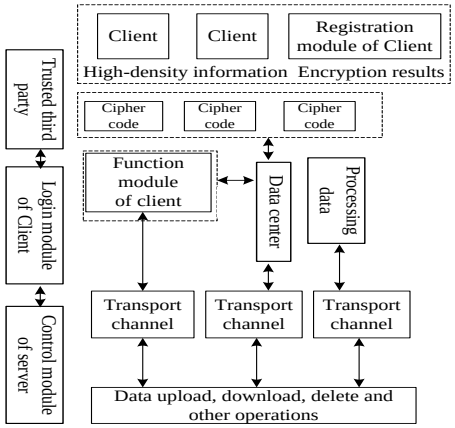


**Fig. 4 Structure of Storage Control Module**

The above is the overall structure design principle of high-density information security storage in big data center. Using this principle, it can complete the overall structure design of high-density information security storage in big data center.

## 3 SECURITY AND POTIMIZATION STORAGE OF HIGH-DENSITY INFORMATION IN BIG DATA CENTER BASED ON FUZZY CLUSTERING

### 3.1 The Primary Feature Extraction of High-density Information Security Storage Space in Big Data Center

In order to improve the accuracy of high-density information security storage in big data centers, the fuzzy theory is firstly used to give the distribution structure of high-density information, and obtain the time series flow model of information security storage and the time interval of high-density data distribution. The information fusion set of the storage space vector is given to obtain the basis function index set of the redundant data in the information storage space. The characteristic distribution gradient index of the time series of high-density information is obtained, and the optimal vector of the hierarchical fusion fuzzy clustering center for security storage of high-density data is given. The specific steps are as follows:

Supposing that $G_1$ and $G_2$ represent the Sink nodes of fuzzy clustering of data storage, $A'_{erp}$ represents the set of transmission vectors in the high-density information acquisition model, $c'_{dgpp}$ represents the edge of the directed graph of the high-density information data distribution, and $R'_{weo}$ represents the sparse characteristics concept set of the sampling time series of high-density information, then the use of formula (1) gives a high-density information distribution structure:

$$E'_{erp} = \frac{R'_{weo} \,\mathrm{m}\, A'_{erp}}{c'_{dgpp}} \otimes \frac{\{G_1 \,\mathrm{m}\, G_2\}}{h'_{uop}} \tag{1}$$

In the above formula, $h'_{uop}$ is an instance set of data information flow.

Assuming that $d'_{dgh}$ is the number of sampling points of high-density information and $n(u)'$ is the characteristic interference in the storage medium, then the time-series flow model of information security storage is calculated using formula (2).

$$A''_{\sup} = \frac{d'_{dgh}}{n(u)'} \pm \{E'_{erp}\} \oplus \frac{a'_{wep} \times x'_{sfjj}}{f'_{etp}} \tag{2}$$

In the above formula, $a'_{wep}$ is the separation measure of data fuzzy clustering, $x'_{sfjj}$ is the oscillation amplitude of the high-density information transmission medium, and $f'_{etp}$ is the structural scale characteristic of the high-density information storage space.

Supposing that $s'_{afh}$ is the scanning time center of the information, $l'_{sgh}$ is the Doppler window length of the information distribution structure, and $x'_{sfg}$ is the decomposition function of the vector quantization feature of high-density information attribute set, then the time interval of high-density data distribution to be stored is obtained by using formula (3):

$$z'_{werj} = \frac{x'_{sfg} \oplus s'_{afh}}{l'_{sgh} \cdot A''_{\sup}} \times \frac{\{c'_{xgjj} \,\mathrm{m}\, g_{lp}\}}{o'_{fhj}} \tag{3}$$

In the above formula, $c'_{xgjj}$ is a fuzzy set of high-density information attribute set, and $g_{lp}$ is the

index value attribute of the user $o'_{fhj}$ in the transmission channel scheduling for high-density information.

Assuming that $\eta'_{wer}$ is the cross-correlation function between the feature vectors of high-density information, $b'_{rtp}$ is the degree of separation measure in the data transmission link layer, $RX$ is the degree of separation measure in the stored information transmission link layer, and $s''_{fg}$ is the constraint function of to satisfy the convergence condition in the discrete sample sampling of the information attribute set to be stored, $e''_{sf}$ is the time series of transmitted data of the high-density information storage space in big data center, then the use of formula (4) gives the information fusion set of storage space vector:

$$D'_{sdp} = \frac{e''_{sf} \, \mathrm{m} \, s''_{fg}}{b'_{rtp}} \oplus \frac{\left\{ RX \, \mathrm{m} \eta'_{wer} \right\}}{x'_{zvjj}} \tag{4}$$

In the above formula, $x'_{zvjj}$ is the vector length of information flow in the storage system.

Supposing that, $s''_{df}$ is the fuzzy convergence control function of information security storage, $\theta'_{sg}$ is the load of the clustering calculation in storage, and $c'_{fg}$ is the clustering attribute of storage data. Then, the formula (5) is used to obtain the base function index set of redundant data in the information storage space:

$$A'_{awe} = \frac{c'_{fg} \otimes \theta'_{sg}}{s''_{df}} \oplus \frac{s''_{sgh} \, \mathrm{m} \, w'_{sgj}}{d'_{dhj}} \pm f'_{fj} \tag{5}$$

In the above formula, $s''_{sgh}$ is the condition that the Sink node needs to satisfy in the information storage system, $w'_{sgj}$ is the decomposition function of vector quantization feature in the data attribute set, and $f'_{fj}$ is the feature fusion center of different high-density information.

Assuming that the $\mathrm{M}'_{wep}$ is the embedding dimension of the data flow fusion in the storage system, $e'_{cf}$ is the set of training sample set of the vector quantization feature decomposition of the high-density information attribute set in the storage space, $\partial'_{dhi}$ is the information fusion set of storage space vector in the big data center, The characteristic distribution gradient index of the high-density information time series is obtained by using formula (6)

$$E'_{wepo} = \frac{\partial'_{dhi} \otimes e'_{cf}}{\mathrm{M}'_{wep} \, \mathrm{m} \, s'_{agi}} \pm \frac{e'_{iop}}{p'_{ghp}} \otimes s'_{shll} \tag{6}$$

In the above formula, $s'_{agi}$ is the weight vector of any training sample, $e'_{iop}$ is the existed high-dimensional eigenvector by the clustering of the data attribute in the information storage medium, and $p'_{ghp}$ is the characteristics of basic frequency in the clustering space of high-density information data, $s'_{shll}$ is the scalar time series in the high-density information set.

Supposing that $e'_{sg}$ is the feature matching set of finite information data set, $df'_{dgj}$ is the main frequency of the high-density information feature, $\varpi'_{pou}$ is the time delay of the data storage, $e'_{swep}$ is the number of samples contained in the each information set, $d''_{cerp}$ is clustering center of the high-density information fusion, then the formula (7) is used to extract the fuzzy membership function of high-density information:

$$J'_{etep} = \frac{e'_{swep} \times df'_{dgj}}{\varpi'_{pou} \times e'_{sg}} \mathrm{m} \frac{d''_{cerp} \otimes g'_{erp}}{p'_{wey}} \tag{7}$$

In the above formula, $g'_{erp}$ is the clustering center of the data fusion, and $p'_{wey}$ is the mean value of the higher order spectral characteristic component of the high-density information.

Assuming that $\varpi'_{oui}$ is the $i$-th vector of the clustering center of high-density information, $x''_{wep}$ is the base function of the high-density information in the data storage center, then the optimal vector of the segmented fusion fuzzy clustering center of high-density information security storage is given by using formula (8):

$$az'_{ryu} = \frac{\left\{ x''_{wep} \oplus \varpi'_{oui} \right\}}{E'_{wepo} \times A'_{awe}} \mathrm{m} \frac{J'_{etep} \, \mathrm{m} \, D'_{sdp}}{A''_{\sup}} \oplus \left\{ z'_{werj} * E'_{erp} \right\} \tag{8}$$

In summary, in the optimization storage process of high-density information security in big data center, the fuzzy theory is used to give the distribution structure of high-density information. The time series flow model of the information security storage is obtained to get the time interval of high-density data distribution to be stored. And the information fusion set of the storage space vector is given, to obtain the base function index set of the redundant data in the information storage space, and the characteristic distribution gradient index of the high-density information time series. The optimal vector of the segmented fusion fuzzy

clustering center of high-density data security storage is proposed to realize the security and optimization storage of high-density information in big data center.

### 3.2 High-density Data Security Storage in the Big Data Center based on the Optimized Tuning

In the security and optimization storage process of high-density information in the big data center, according to the optimal vector of the segmented fusion fuzzy clustering center of $az'_{ryu}$ obtained in section 3.1, and the high-density information is made composite chaotic encryption. The correlation coefficient and uniformity index are used to construct the integrated objective function of high-density information security storage. The control parameter of the complex chaotic cryptosystem are coordinated, optimized and adjusted to improve and perfect the function of high-density information security storage in big data center. Specific steps are described below:

Supposing that $x'_{sfg}$ is the chaotic variable, $\mu'_{opi}$ is the control parameter, according to the optimal vector of the segmented fusion fuzzy clustering center of $az'_{ryu}$ obtained in section 3.1, in wavelet transformation space, the wavelet coefficient of plaintext is made composite encryption, using formula (9) to describe:

$$Z'_{asr} = \frac{\mu'_{opi} \oplus x'_{sfg}}{az'_{ryu}} \oplus \frac{\left\{ z'_{per} \otimes c'_{erp} \right\}}{j'_{wkp} \,\mathrm{m}\, c'_{werp}} \tag{9}$$

In above formula, $z'_{per}$ stands for the analytic equation of the Logistic mapping of high-density information security storage, and $c'_{erp}$ is the pseudo-random sequence.

Supposing that, the controllable parameter of chaotic encryption is represented by $\mu$, $E'_{swer}$ is the presented initial chaos status of the system, $\psi(t)$ is the basic wavelet function, to impel $\psi(t)$ by the scale expansion and translation transform to generate function clusters, represented by $\psi_{\varepsilon,\tau}(t)$. The formula (10) is used to form chaotic cipher sequence:

$$Z'_{weghr} = \frac{\psi_{\varepsilon,\tau}(t) \,\mathrm{m}\, \psi(t)}{E'_{swer} \oplus \mu} \oplus \frac{d'_{sgj} \,\mathrm{m}\left\{ X_{C1}, X_{C2} \right\}}{T_{C1} \,\mathrm{m}\, T_{C2}} \oplus u(n) \tag{10}$$

In the upper model, $d'_{sgj}$ is the control parameter that represents the difference characteristics of chaotic motion. $X_{C1}$ and $X_{C2}$ respectively represent one-dimensional discrete chaotic sequence generated by the iteration, $T_{C1}$ and $T_{C2}$ respectively represent delay time constant, and $u(n)$ represents jump function.

It is assumed that, $X_n$ is the length of the wavelet sequence of the plaintext information, the wavelet coefficient of plaintext information represented by $X_{sw}$ is obtained, and the wavelet transform sequence $X_{swt}$ is obtained by proportional transformation. The ciphertext sequence $v'_{cbnm}$ is generated by using formula (11):

$$v'_{cbnm} = \frac{K_C \oplus X_{st}}{\left\{ K_1, K_2 \right\}} \otimes \frac{K_3}{Z'_{weghr}} \,\mathrm{m}\, X_{ce} \tag{11}$$

In the upper model, $K_1$ and $K_2$ represent the cipher codes, $K_3$ is the block of cipher codes, and $X_{ce}$ is the encryption block sequence of complex chaotic equaled with the length of $X_{swt}$.

Assuming that $L_S$ is the length of wavelet sequence $X_n$ of plaintext information, the length is defined as the adaptive value of the current ciphertext sequence $v'_{cbnm}$, $P'_{SDE}$ is the constraints of the preset threshold, and using the formula (12) determine whether the $L_S$ meets the constraints of preset threshold:

$$s'_{dfy} = \frac{\partial_{uip} \pm p'_{kop} \le L_S}{v'_{cbnm} \,\mathrm{m}\left\{ p'_{kop} \ge L_S \right\}} P'_{SDE} \otimes \left\{ X_n \right\} \tag{12}$$

In the formula, $p'_{kop}$ represents the concealment of plaintext information, and $\partial_{uip}$ stands for an important index to measure the ability of anti-attack and anti-break of cipher system.

Assuming that, $\kappa'_{poi}$ stands for the sensitivity of the chaotic motion system to the initial encryption system, and the uniformity represented by $\omega'_{wer}$ is introduced to make quantitative evaluation of the uniform distribution of encrypted information. Formula (13) is used to take the correlation coefficient and the evenness index, to construct the comprehensive target function of high-density information security storage:

$$Z'_{GYU} = \frac{U_{nif} \times \kappa'_{poi}}{\mu'_{dry} \times V'_{erp}} \oplus \omega'_{wer} \tag{13}$$

In the formula, $U_{nif}$ is the normalized similarity function, $\mu'_{dry}$ is the weights of normalized

similarity function, $\mu'_{dry}$ is used to measure the degree of similarity between the ciphertext sequence and the plaintext sequence, $V'_{erp}$ is the difference of the motion characteristics in one-dimensional chaotic system.

It is assumed that $\mu'_{iou}$ is the cross correlation coefficient between the ciphertext sequence and the plaintext sequence, $\{a_1, a_2\}$ is the weight coefficient, and $f'_{iou}$ is the homogeneity of the ciphertext sequence, then the formula (14) is used to complete the security storage of the high-density information in the big data center:

$$W'_{SF} = \frac{\mu'_{iou} \pm \{a_1, a_2\}}{f'_{iou}} \mathrm{m}\, z'_{sfgh} \otimes f'_{fhk} \qquad (14)$$

In the above formula, $z'_{sfgh}$ stands for the attenuation coefficient of encryption performance of the complex chaotic cryptosystem, and $f'_{fhk}$ represents that the composite chaotic system has a stronger initial sensitivity.

## 4 EXPERIMENT AND SIMULATION PROOF

In order to prove the validity of the proposed method based on fuzzy clustering for high-density data security storage in big data center, an experiment is needed. C + + and Matlab7 mixed programming simulation platform is used. The hardware environment of the experiment is: Intel (R) Core (TM) 2Duo CPU, 2.94GHz, 4GB memory, Windows 7 operating system. The time interval of the data characteristics acquisition is 0.25s and the frequency of characteristics sampling $f_s = 4$, $f_0 = 20kH_z$. The length of time series sampling of a single set of high-density information is 140, the range of expanded bandwidth change in a data storage system is 1~10db, and the maximum number of iterations is $NP = 29$. In the experiment, the one set of high-density information with different attributes are taken as sample, to obtain the time series waveform of the sample testing set of data storage shown as figure 5.

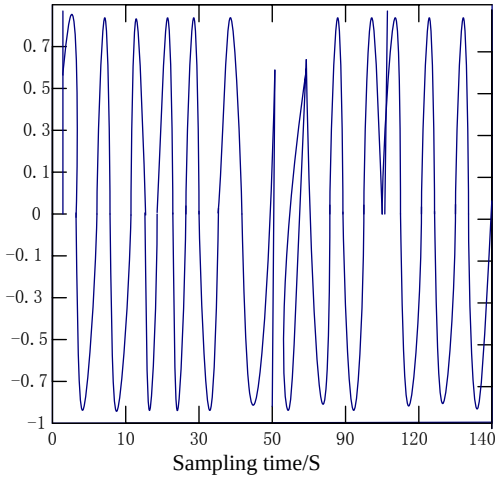


**Fig. 5 Time Series Waveform of Sample Testing Set of High-density Information Storage**

### 4.1 The Establishment of Evaluation Indexes

In order to verify the feasibility of the proposed method, the experiment is divided into two different stages. In the first stage of the experiment, the storage security is used as an evaluation index to test the performance of the proposed method for high-density data security storage in big data center. In the second stage of the experiment, in order to show the comprehensiveness and impartiality of the experiment, the above results are compared with the method used in the (Wu, Wang, Liang, et al.2016). The throughput performance of storage system is used to verify the effectiveness of different methods for high-density information security storage in big data center.

### 4.2 Storage Security Test of the Proposed Method

Using the fuzzy clustering method proposed in this paper, the high-density information security storage experiment in big data center is carried out, and the security of this method is tested. The result is shown in figure 6.

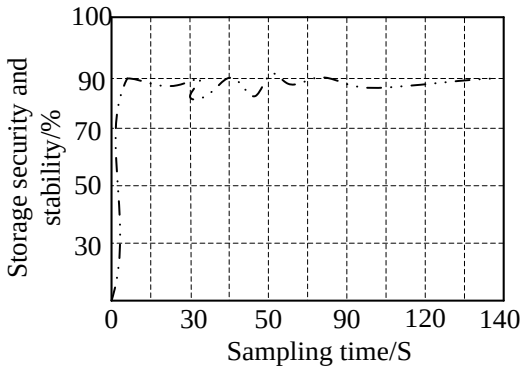


**Fig. 6 Security and Stability of Storage by the Proposed Method**

The simulation results in figure 6 shows that with the increase of the sampling time, the security and stability of using this method for high-density information security storage in big data center always higher, which can fully meet the needs of security and stability of high-density information security storage in big data center.

### 4.3 Comparison of Throughput Performance of Storage System by Different Methods

Using the proposed method and the method of (Wu, Wang, Liang, et al. 2015), the experiment for high-density information security storage in big data center is carried out. the throughput performance of high-density information security storage in big data center by different methods is compared, and the results are shown in figure 7.

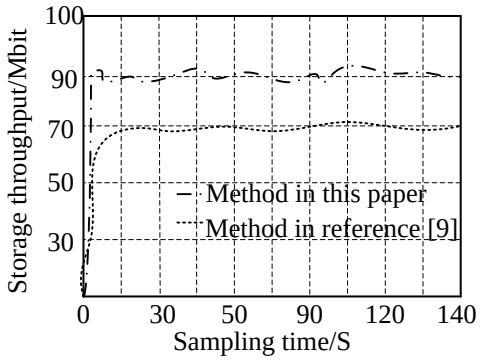


**Fig. 7 Throughput Performance of Storage by Different Methods**

The simulation experiment results in figure 6 show that with the increase of the sampling time, the throughput of using the proposed method for high-density information security storage in the big data center has obvious advantages compared to that of the method in (Wu et al. 2016), it greatly enhances the quality of high-density information security storage in the big data center.

Experimental results show that the proposed method has higher security and stability for data storage, and is of great significance to the security of network information.

## 5 CONCLUSION

In this paper, the problem of high-density information security storage in big data center is studied. the grid distribution structure model of data security storage is established and vector quantization characteristics of the high-density information attribute set are decomposed. In order to improve the security of high-density information storage, the segmented matching detection method is applied to compact features for the stored data flow. Experimental results show that the proposed method has higher security and stability for data storage, and is of great significance to the security of network information.

**Acknowledgement**

This paper was supported by (1) The 2016 Science and Technology Project of the Education Department Of Fujian Province, "Design and Implementation of a Data Mining System Based on Teaching Evaluation" (JA114145); (2)The 2018 science and technology project of Fujian Chuanzheng Communications College, "Research on the Construction of a Vehicle-free Carrier Monitoring System Based on Internet plus" (X19107001).

## REFERENCES

Banihani R, Harb S, Mhaidat K, et al. High-Throughput and Area-Efficient FPGA Implementations of Data Encryption Standard (DES)[J]. *Circuits & Systems*, 2014, 5(3):45-56.

CHA Zhiyong,LUO Xian,LIU Feng,et al.False information filtering methods in intelligent sensor optimization research[J]. *Computer Simulation*, 2016, 33(12):249-252.

Chen H, Du X, Liu Z. Optical hyperspectral data encryption in spectrum domain by using 3D Arnold and gyrator transforms[J]. *Spectroscopy Letters*, 2016, 49(2):103-107.

Chen S, Zhong X X. Research of Cipher Chip Core for Sensor Data Encryption[J]. IEEE Sensors Journal, 2016, 16(12):4949-4954.

Du N, Manjunath N, Shuai Y, et al. Novel implementation of memristive systems for data encryption and obfuscation[J]. *Journal of Applied Physics*, 2014, 115(12):124117-279.

Jo H, Hong S T, Chang J W, et al. Offloading data encryption to GPU in database systems[J]. *The Journal of Supercomputing*, 2014, 69(1):375-394.

Kaczmarczyk V, Bradáč Z, Fiedler P, et al. Client side data encryption/decryption for web application[J]. *IFAC-PapersOnLine*, 2016, 49(25):241-246.

Kumar S, Srivastava S. Image Encryption using Simplified Data Encryption Standard (S-DES)[J]. *Information Age*, 2014, 9(2):46-2.

Mahna S, Ch S. Data Encryption Techniques for USB[J]. International Journal of Computer Applications, 2014, 104(7):14-17.

MIN Xiaozhong,ZHU LinliDesign of Reconciliation Algorithm Based on Large Data[J].

*Science Technology and Engineering* , 2014, 14(24):248-251.

Nagaraj S, Raju G S V P, Srinadth V. Data Encryption and Authetication Using Public Key Approach ☆[J]. *Procedia Computer Science*, 2015, 48:126-132.

NIU Geng.Improved Large Data Stratification Contribution KNN Clustering Algorithm[J]. *Bulletin of Science and Technology*, 2015, 31(8):129-131.

Ottoy G, Hamelinckx T, Preneel B, et al. On the choice of the appropriate AES data encryption method for ZigBee nodes[J]. *Security & Communication Networks*, 2016, 9(2):87-93.

Srichavengsup W, Sanum W. Data Encryption Scheme Based on Rules of Cellular Automata and Chaotic Map Function for Information Security[J]. *International Journal of Network Security*, 2016, 18(6):1130-1142.

Tsai K L, Leu F Y, Tsai S H. Data encryption method using environmental secret key with server assistance[J]. *Intelligent Automation & Soft Computing*, 2016, 22(3):1-8.

Tsai K L, Leu F Y, Tsai S H. Data encryption method using environmental secret key with server assistance[J]. *Intelligent Automation & Soft Computing*, 2016, 22(3):1-8.

Wanpeng. Adaptive and Dynamic Mobile Phone Data Encryption Method[J]. *China Communications*, 2014, 11(1):103-109.

Wu J, Wang W, Liang Q, et al. Compressive sensing- based data encryption system with application to sense-through-wall UWB noise radar[J]. *Security & Communication Networks*, 2016, 9(5):371-379.

YANG Fei,XIAO ManshengRegression Based Power-efficient Data Streams Aggregation Algorithm[J].*Computer Measurement & Control* , 2015, 23(2):508-511.

ZHOU Xiaojuan.Implementation of lightweight big data analysis system[J]. *Electronic Design Engineering*, 2016, 24(8):40-43.