International Journal of Security and Its Applications
Vol. 10, No. 9 (2016), pp.77-86
http://dx.doi.org/10.14257/ijsia.2016.10.9.09

Evaluation Model of Cloud Storage Security Level with the Fusion Analytic Hierarchy Process

Cheng Cheng[1] and Zhou Enyi[2]

[1]*School of management, Xi'an University of Architecture and Technology, Xi'an, China*
[2]*Xi'an University of Architecture and Technology, Xi'an, China*
chengcheng0403@163.com

Abstract

In view of excessive calculation and bandwidth cost, excessive complexity of the user access permission revocation in the cloud storage service, taking the ciphertext access control scheme of property encryption system (CP - ABE) of ciphertext strategy as the theoretical background, this article designed a cloud storage permission revocation optimization mechanism based on the dynamic re-encryption, namely DRPRO. The mechanism uses (k, n) threshold scheme to divide data information into several blocks, and dynamically selects a data information block to implement the re-encryption, and completes the user access permission revocation realization process by data partitioning, reconstruction, transfer, extraction, permission revocation and other subalgorithm successively. Theoretical analysis and simulation experiment evaluation show that under the premise of ensuring the high security of cloud storage service user data, DRPRO mechanism reduces the calculation and bandwidth cost of the user access permission revocation effectively, and its performance efficiency has been further optimized and improved.

Keywords*: Cloud storage; Ciphertext access control; Safety evaluation; Permission revocation; Dynamic re-encryption*

1. Introduction

At present, the global information technology experts have carried out a great deal of experimental studies, such as the complete re-encryption technology pointed out in the reference[1], the encryption technology is completely established on the revocation mechanism of access permission, and the system re-encrypts the user data information automatically before the users upload data to the cloud storage servers. When the user exercises the permission to change the rights, the users themselves re-encrypt the data information uploaded again. Thus, although the security of storage information in the cloud storage server is ensured, the complete re-encryption technology also improves the requirements for the user calculation and bandwidth, bringing new problems to the development of cloud storage service. This article took the CP - ABE ciphertext access control technology as the original plan on the above problems, and developed the cloud storage permission change mechanism of the dynamic control re-encryption, namely DRPRO. The mechanism uses (k, n) threshold scheme to divide storage data into several blocks, dynamically selects a data information block to re-encrypt, and implements the user access permission revocation after performing the data partitioning transmission, reconstruction and other steps. Through a great deal of theoretical research and experimental data validation, DRPRO mechanism can greatly reduce the high requirements for calculation and bandwidth caused by the user changing access permission under the premise of ensuring the high security of cloud storage service data, to implement the significant improvement of working efficiency.

ISSN: 1738-9976 IJSIA

2. DRPRO Mechanism

2.1. Dynamic Control Re-encryption

Dynamic control re-encryption technology is an encryption mechanism between complete re-encryption and lazy re-encryption, bringing the advantages of the two encryption technologies together, and specific encryption principle is as follows:

The operation technology of various encodings is summarized to divide the whole storage data F into n parts of different data blocks, and then the data block is uploaded to the cloud storage server; First the data block F is re-encrypted, one storage data block is dynamically extracted to carry out the operation, which is used to replace the re-encrypted data file. As shown in Figure 1. Thereinto, non-dynamic data represents the unencrypted data in the F, but on the contrary, dynamic data represents the data in the F which must be re-encrypted.

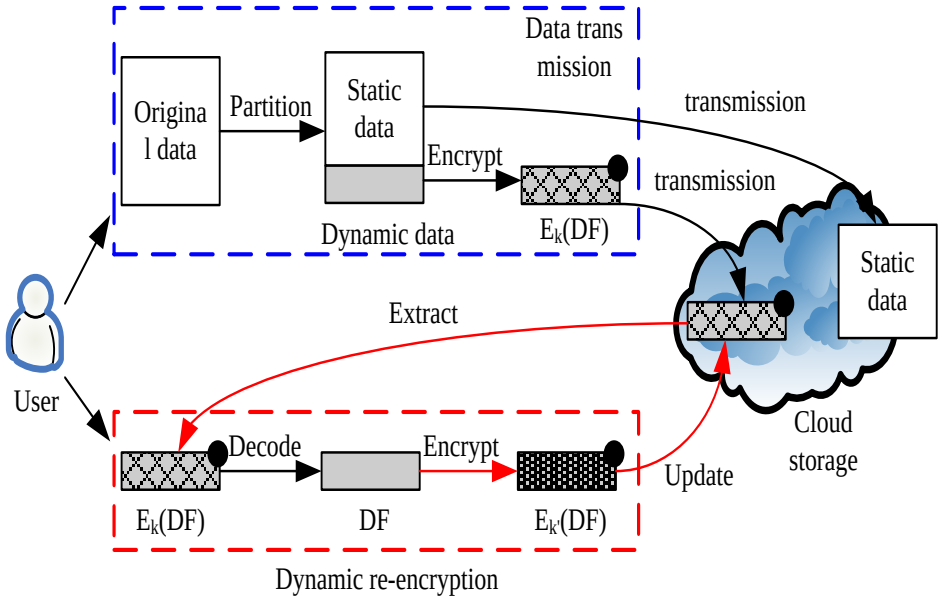

Figure 1. Dynamic Re-encryption Basic Process Framework

2.2. Cloud Storage Permission Change and Optimization Algorithm

Taking CP-ABE ciphertext access control technology as the original plan, dynamic control re-encryption mechanism is tested through relevant data process subalgorithm, and the user access permission change process is implemented through data partitioning, reconstruction, data upload, permission change and other subalgorithm.

2.2.1. Data Partitioning: For the information encoding mechanism put forward in the reference[14], the data dispersal algorithm in reference [13] carries out the practice verification. First of all, the information coding mechanism put forward in the reference [14] conducts the encoding operation on the data file F; Secondly, the data dispersal algorithm in the reference [13] is used to divide the encoding operation result of data F into N parks of different data blocks. If the data information F has 7 bytes and the byte length is W bits, E represents data key encryption algorithm, and its data partitioning subalgorithm pseudo code is as follows:

Algorithm 1: Data partitioning
Input: data file $F: m_1, m_2, \cdots, m_t$; Data partitioning size: n
Output: key information K_1, data block: $s_1, s_2, \cdots, s_n$
1. Calculate the integrity measurement parameter $m_{t+1} = hash(m_1, m_2, \cdots, m_t)$ of F; 2. Select the temporary key information K, used for encryption operation of E; 3. Encoding operation: $c_i = m_i \oplus E_k(i)$, and $1 \le i \le t+1$; 4. Obtain key information $K_1 = K \oplus h_1 \oplus h_2 \oplus \cdots \oplus h_{t+1}$, and $h_i = hash(c_i)$ 5. Link encoding operation result, which is regarded as the input parameter of (n, n) threshold scheme; 6. Perform the data dispersal algorithm in the reference [13], and output n parts of different shared data blocks $s_1, s_2, \cdots, s_n$.

The operation result c_{t+1} of the data encoding can be directly used on the checking the data integrity. In terms of theory, the data partitioning scheme is (n, n) threshold optimization scheme.

2.2.2. Data Reconstruction: If the data partitioning subalgorithm is operated in reverse, the data reconstruction subalgorithm can be obtained, and its data reconstruction subalgorithm pseudo code is as follows:

Algorithm 2: Data reconstruction
Input: key information K_1, data blocks: $s_1, s_2, \cdots, s_n$
Output: data file $F: m_1, m_2, \cdots, m_t$; Data partitioning size: n

1. Obtain all data blocks $s_1, s_2, \cdots, s_n$, perform the data dispersal algorithm in the reference [13] and reconstruct data file F;
2. Partition and reconstruct data information: $c_1, c_2, \cdots, c_t, c_{t+1}$;
3. Obtain key information $K = K_1 \oplus h_1 \oplus h_2 \oplus \cdots \oplus h_{t+1}$, and $h_i = hash(c_i)$;
4. Encoding reverse operation: $m_i = c_i \oplus E_k(i)$, and $1 \le i \le t+1$;
5. Obtain $m'_{t+1} = hash(m_1, m_2, \cdots, m_t)$;
if $m'_{t+1} \ne m_{t+1}$ *then*
Data reconstruction fails;
else
9. The data reconstruction is successful, and output the data file $F: m_1, m_2, \cdots, m_t$;
end if

2.2.3. Data Transmission: After data file F is divided, it is uploaded to the cloud storage server and must be implemented through data transfer subalgorithm, and its algorithm pseudo code is as follows:

Algorithm 3: Data transmission subalgorithm
Input: data file $F: m_1, m_2, \cdots, m_t$; Data partitioning size: n Output: data storage location uses the URL logo to describe
Perform data partitioning subalgorithm, and obtain key information K_1 and shared data blocks $s_1, s_2, \cdots, s_n$ 2. Select the one $s_i, (1 \le i \le n)$ as the dynamic data; 3. Select some key information K_2; 4. Perform $E_{k_2}(s_i)$; 5. Perform $E'_T(K_1 + K_2)$, E' represents a cloud storage ciphertext algorithm based on CP - ABE, and T represents the access control model of data information; 6. $E'_T(K_1 + K_2)$, $E_{k_2}(s_i)$ and $s_1, s_2, \cdots, s_{i-1}, s_{i+1}, \cdots, s_n$ are uploaded to cloud storage server; 7. Output URL logo corresponding to the data result of step 6.

2.2.4. Data Extraction: The initial data information file F has been encrypted, and then is uploaded to the cloud storage server, URL logo conducts the data retrieval directly, and all data users can get URL logo, however, only the data users meeting the permission can decrypt and extract the original data file F. Its data extraction subalgorithm pseudo code is as follows:

Algorithm 4: Data extraction
Input: user private key information SK and URL logo Output: data file $F: m_1, m_2, \cdots, m_t$
According to URL logo, get $E'_T(K_1 + K_2)$, $E_{k_2}(s_i)$ and $s_1, s_2, \cdots, s_{i-1}, s_{i+1}, \cdots, s_n$; 2. If SK characteristic set S does not meet the access control structure T, then 3. Data extraction fails; 4. *end if* 5. Perform $E'_T(K_1 + K_2)$, and obtain the key information K_1 and K_2; 6. Perform $E_{k_2}(s_i)$, and obtain s_i; 7. According to K_1 and $s_1, s_2, \cdots, s_n$, perform data reconstruction subalgorithm; 8. If data reconstruction fails, then 9. Data extraction fails; 10. *else* 11. Data extraction is successful, and output data file $F: m_1, m_2, \cdots, m_t$; 12. *end if*

After the data information file F is uploaded to the cloud storage server, the user has to download the access control structure T corresponding to the latest data file F for some reason, and the user permission must be used to carry out the authorization operation at this time.

2.2.5. Permission Revocation: The re-encryption permission revocation process which completes the dynamic control is more tediou, first the users must extract $E'_T(K_1+K_2)$, dynamic data is re-encrypted, and the required dynamic data is obtained randomly. Its algorithm pseudo code is as follows:

Algorithm 5: Permission revocation
Input: access control structure T' of data file F, URL logo

On the basis of URL logo, obtain $E'_T(K_1+K_2)$ and $E_{k_2}(s_i)$
Perform $E'_T(K_1+K_2)$, and obtain the key information K_1 and K_2;
Perform $E_{k_2}(s_i)$, and obtain s_i;
Select the temporary key information K;
Set $K_2 = K$, and perform $E'_T(K_1+K_2)$;
Select a temporary logo j, $j \in [1,\cdots,n]$;
if $i \neq j$ *then*
On the basis of URL logo, obtain s_j;
Perform $E_{k_2}(s_j)$
10.Update $E'_T(K_1+K_2)$, s_i and $E_{k_2}(s_j)$ to the cloud storage server, and remove the original data information $E'_T(K_1+K_2)$, $E_{k_2}(s_i)$, s_j;
else
Perform $E_{k_2}(s_i)$
Update $E'_T(K_1+K_2)$, $E_{k_2}(s_i)$ to the cloud storage server, and remove the original data information $E'_T(K_1+K_2)$ and $E_{k_2}(s_i)$;
14. *end if*

3. Experiment

3.1. Experiment Evaluation

The comprehensive performances of permission revocation mechanism obtained from the reference [1] and the reference [2] are compared. Assuming that the 100 MB data information file F is divided into 10 blocks, and the encoding speed of (n,n) threshold scheme is 50 MB per second, with $N = 13107200$, $n = 10$, $E_{ida} = D_{ida} = 50$, and the analysis comparison of comprehensive performance is conducted on the dynamic control re-encryption DRPRO mechanism and permission revocation mechanism the reference [1] and [2] reference give, shown in Figure 4.

We can get from Figure 2 that the dynamic control re-encryption DRPRO mechanism is the middle scheme of permission revocation mechanisms obtained from the reference [1] and reference [2]. The comprehensive performance of DRPRO mechanism is far above the proposed scheme in the reference [1] on the permission revocation step, even though the proposed scheme in the reference [2] reduces the user calculation and bandwidth requirements, its safety performance is not ideal. Although the processing data time of DRPRO mechanism is slightly longer in the process of data upload and interception, it not only has improved the data partitioning and reconstructed the processing mechanism, but also has reduced its calculation and bandwidth requirements.

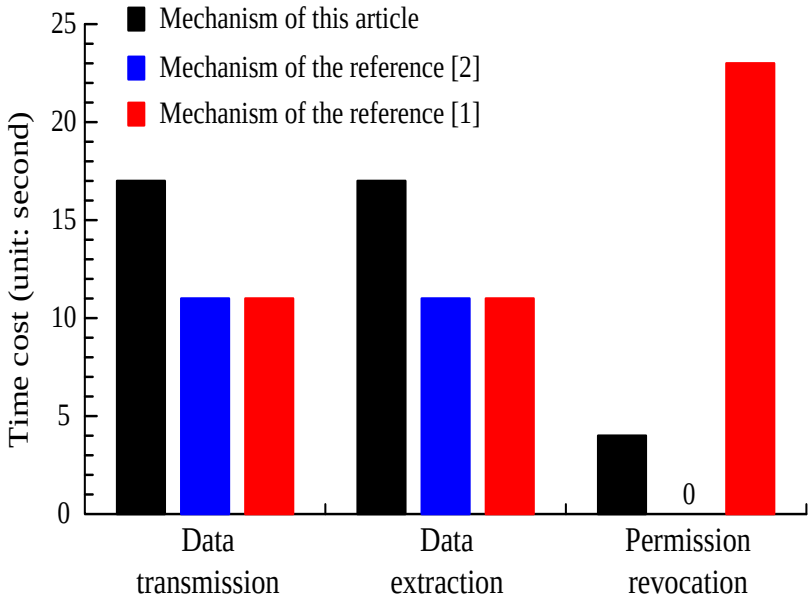

Figure 2. Optimization Performance Comparison under Different Links

Total user time cost is the sum of data transfer and permission revocation time cost, as follows:

$$T_{manage} = T_{transfer} + T_{revoke} \tag{6}$$

Setting x represents the number of re-encryption, when a certain threshold x_i is reached, DRPRO mechanism optimization ability is shown. As shown in Figure 3.

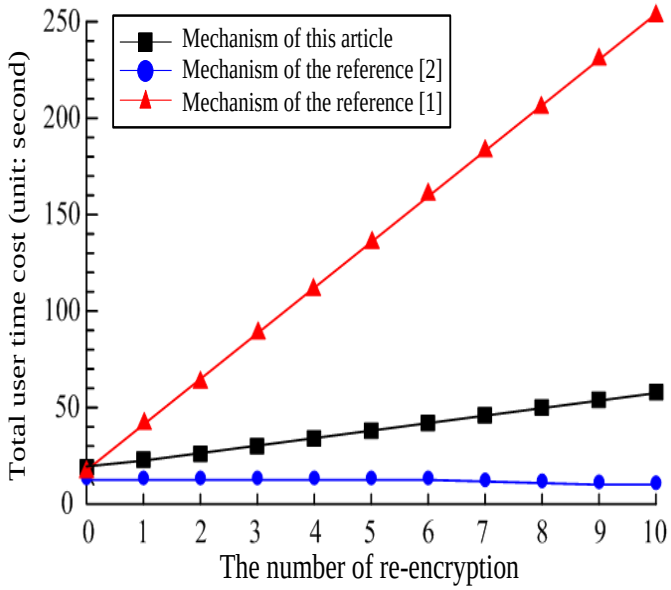

Figure 3. Total User Time Cost Comparison under the Condition of Different Re-encryption Times

3.2. Analysis of Experimental Results

First of all, the developed CP - ABE ciphertext cloud storage platform based on the C++ tests the comprehensive performance of DRPRO mechanism, and the platform operates under Linux system. Some algorithm needs to be applied in the test phase, such as AES - 192, SHA - 256; CP - ABE tool library [15] still needs to be added, to complete CP - ABE encryption; Information partitioning algorithm and open source example must be combined to successfully apply (n, n) threshold scheme.

The terminal running program and the client running program constitute the operation platform of the testing experiment together, and the user's data transfer and permission revocation are implemented when the terminal running program is completed; The user's data interception is implemented when the user's running client program is completed. CP- ABE algorithm is implemented at terminal, the terminal running program and the client running program can be done with a single thread, and cloud storage platform applies HDFS on the Hadoop, to implement running on Ubuntu system. The basic configuration of experimental test equipment is as shown in Table 1.

Table 1. Experimental Equipment Configuration Required

Experimental equipment	Basic configuration
Server and client	■ Quad-Core Intel CoreTM Q6600 processor ■ 2.40GHz processor ■ 8MB processor cache ■ 2GB memory capacity
HDFS Storage	■ 4 core Intel Xeon E5506 processor ■ 2.13GHz processor basic frequency ■ 4MB processor cache ■ 4GB memory capacity ■ 1TB Xijie serial hard disk
Internetwork	■ 1000 Mbps Ethernet card ■ 100 Mbps interchanger

The re-encryption mechanism which is put forward in the reference [1] and in the reference [2] and still used and DRPRO encryption mechanism of this article are compared. Now two experiment conditions are analyzed below. As shown in Figure 4, 5.

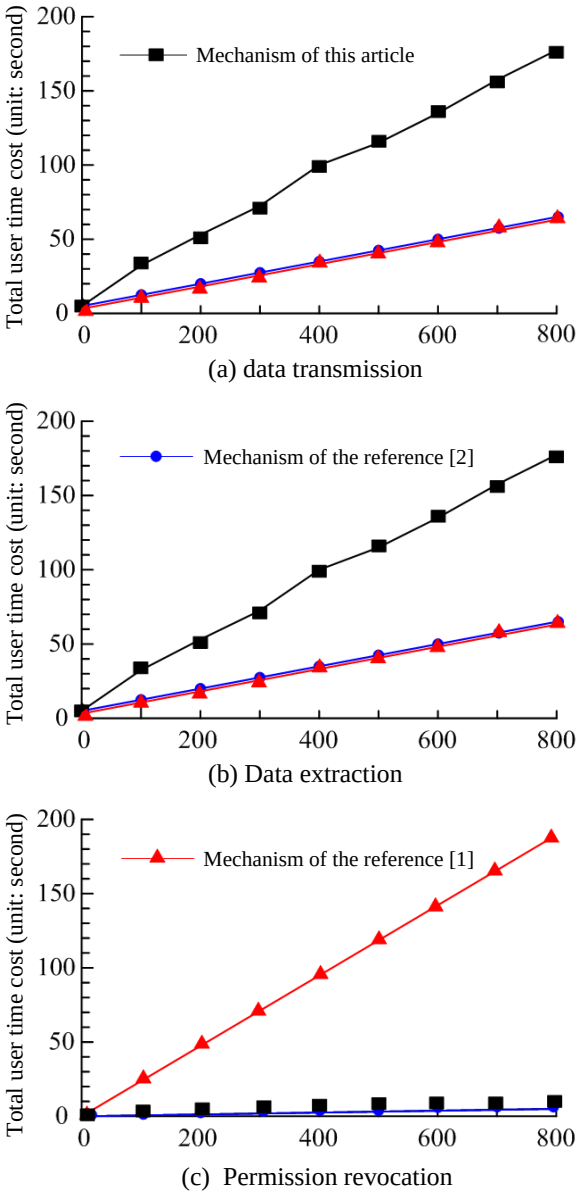

Figure 4. Mechanism Performance Comparison under the Change of the Data File F

(1) The memory of data information file F gradually becomes larger, and data block volume is constant. We can draw from figure 6, the deficiencies of DRPRO mechanism is that the requirement of calculation and bandwidth is higher than the re-encryption mechanism requirement proposed in the reference [1] and in the reference [2] when the user data transfer and data extraction are conducted, its advantage is that the requirement of calculation and bandwidth is lower than the re-encryption mechanism requirement proposed in the reference [1] on the permission revocation link.

(2) The memory of data information file F is constant, and data block volume gradually becomes larger. We can draw from figure 7, when the number of partitioning the shared data blocks increases, the number of files increases gradually, the permission revocation cost of re-encryption mechanism proposed in the reference [1] remains high,

while the permission revocation cost of DRPRO mechanism gradually declines, and the performance is further optimized.

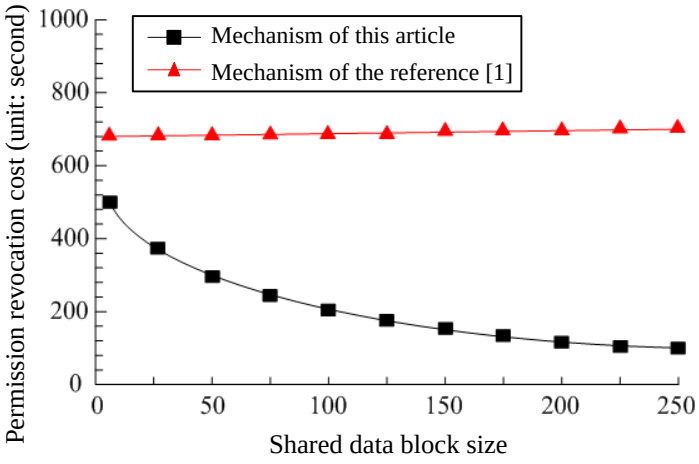

Figure 5. Mechanism Performance Comparison under the Change of the Shared Data Block

4. Conclusion

To solve the problems of higher calculation and bandwidth cost, complexity of user access permission revocation in the cloud storage service, taking the CP-ABE ciphertext access control technology scheme as the original scheme, this article carried out the study and obtained the dynamic re-encryption DRPRO permission revocation optimization mechanism. This mechanism applied (k, n) threshold scheme, to divide the data information into n blocks, a data information block is extracted randomly for re-encryption, then data partitioning, reconstruction, data transfer, data extraction and permission revocation and other operation are carried out in turn, and the user permission revocation is implemented through the above steps. Through the analysis of its safety performance, the safety performance of DRPRO encryption mechanism on the process of encrypted file and the dynamic control re-encryption is higher. Through the comprehensive performance analysis and practice verification, DRPRO encryption mechanism significantly reduces the bandwidth requirement of the calculation and bandwidth of user access permission revocation. Compared with other re-encryption mechanisms, its comprehensive performance and work efficiency are improved significantly.

References

[1] G. Bao, L. Mi, Y. Geng and K. Pahlavan, "A computer vision based speed estimation technique for localizing the wireless capsule endoscope inside small intestine", 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), **(2014)** Aug.
[2] X. Song and Y. Geng, "Distributed community detection optimization algorithm for complex networks", Journal of Networks, vol. 9, no. 10, **(2014)** Jan., pp. 2758-2765.
[3] Jiang D., Ying X. and Han Y., "Collaborative multi-hop routing in cognitive wireless networks[J]", Wireless Personal Communications, **(2015)**, pp. 1-23.
[4] J. Hu and Z. Gao, "Modules identification in gene positive networks of hepatocellular carcinoma using Pearson agglomerative method and Pearson cohesion coupling modularity[J]", Journal of Applied Mathematics, 2012 **(2012)**.
[5] Jiang D., Xu Z. and Chen Z., "Joint time-frequency sparse estimation of large-scale network traffic[J]", Computer Networks, vol. 55, no. 15, **(2011)**, pp. 3533-3547. J. Hu, Z. Gao and W. Pan, "Multiangle

Social Network Recommendation Algorithms and Similarity Network Evaluation[J]", Journal of Applied Mathematics, 2013 **(2013)**.
[6] M. Zhou, G. Bao, Y. Geng, B. Alkandari and X. Li, "Polyp detection and radius measurement in small intestine using video capsule endoscopy", 2014 7th International Conference on Biomedical Engineering and Informatics (BMEI), **(2014)** Oct.
[7] G. Yan, Y. Lv, Q. Wang and Y. Geng, "Routing algorithm based on delay rate in wireless cognitive radio network", Journal of Networks, vol. 9, no. 4, **(2014)** Jan. pp. 948-955.
[8] Lin Y., Yang J. and Lv Z., "A Self-Assessment Stereo Capture Model Applicable to the Internet of Things[J]", Sensors, vol. 15, no. 8, **(2015)**, pp. 20925-20944.
[9] Wang K., Zhou X. and Li T., "Optimizing load balancing and data-locality with data-aware scheduling[C]", Big Data (Big Data), 2014 IEEE International Conference on. IEEE, **(2014)**, pp. 119-128.
[10] Zhang L., He B. and Sun J., "Double Image Multi-Encryption Algorithm Based on Fractional Chaotic Time Series[J]", Journal of Computational and Theoretical Nanoscience, vol. 12, **(2015)**, pp. 1-7.
[11] Su T., Lv Z. and Gao S., "3d seabed: 3d modeling and visualization platform for the seabed[C]", Multimedia and Expo Workshops (ICMEW), 2014 IEEE International Conference on. IEEE, **(2014)**, pp. 1-6.
[12] Y. Geng, J. Chen, R. Fu, G. Bao and K. Pahlavan, "Enlighten wearable physiological monitoring systems: On-body rf characteristics based human motion classification using a support vector machine", IEEE transactions on mobile computing, vol. 1, no. 1, **(2015)** Apr., pp. 1-15.
[13] Lv Z., Halawani A. and Feng S., "Multimodal hand and foot gesture interaction for handheld devices[J]", ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 11, no. 1s, **(2014)**, p. 10.
[14] G. Liu, Y. Geng and K. Pahlavan, "Effects of calibration RFID tags on performance of inertial navigation in indoor environment", 2015 International Conference on Computing, Networking and Communications (ICNC), **(2015)** Feb.
[15] J. He, Y. Geng, Y. Wan, S. Li and K. Pahlavan, "A cyber physical test-bed for virtualization of RF access environment for body sensor network", IEEE Sensor Journal, vol. 13, no. 10, **(2013)** Oct., pp. 3826-3836.
[16] W. Huang and Y. Geng, "Identification Method of Attack Path Based on Immune Intrusion Detection", Journal of Networks, vol. 9, no. 4, **(2014)** Jan., pp. 964-971.
[17] Li X., Lv Z. and Hu J., "XEarth: A 3D GIS Platform for managing massive city information[C]", Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2015 IEEE International Conference on. IEEE, **(2015)**, pp. 1-6.

Authors

Cheng Cheng, is a PhD at the Xi'an University of Architecture And Technology. Her major is management science and engineering, and the research direction is the optimization and management of human resources system.

