ISBN: 978-981-14-2136-5

Multi-level Security Task Scheduling Scheme Based on Task Priority

LI Li[1, 2], SHI Guozhen[1], LI Xuemei[1], WANG Xuan[2]

[1]Beijing Electronics Science and Technology Institute; [2]Xidian University
[1]No. 7, Fufeng Road, Fengtai District, 100070; [2]No. 2, Taibai South Road, Yanta District, 710071
[1]Beijing, China; [2]Xi'an, Shaanxi, China
laury_li@126.com, sgz1974@163.com, lixuemei@besti.edu.cn

Abstract

Data security is a primary consideration when users choose cloud storage, and it is also an important factor that hinders the development of cloud storage. In order to meet the requirements of secure storage of user-differentiated data and guarantee a good user service experience, we propose a multi-level security task scheduling scheme that comprehensively considers the data security level, user service level, and task waiting time. The scheme adopts the idea of multi-level security. The security requirements of different security level data are ensured by the key strength of the cryptographic algorithm. The mapping between the data security level and the key length under the selected cryptographic algorithm achieves the task's priority order. Scheduling appropriate encryption modules to implement differentiated encryption is suitable for cloud storage environments where data sensitivity and importance are diversified.

Key words: multi-level security, data security level, key length, task scheduling; priority

Introduction

Under the background of big data, with the increase of the scale of corporate and personal data, cloud storage provides new options for data storage and backup. At present, many users choose to save files on the cloud, such as Amazon AWS, Google Drive, Windows Azure, Ali cloud, Tencent cloud, Baidu cloud and so on. Compared with traditional storage methods, cloud storage has many advantages, namely, cost savings, easy expansion of storage capacity, easily accessed by computers, mobile phones, and other terminals at any place that can be connected to the Internet. However, cloud storage also faces some potential security threats. According to the analysis given by well-known organizations such as ENISA, Gartner, and CSA, issues such as data security and tenant isolation are among the top issues. Among the "Twelve Cloud Security Threats" listed by the Cloud Security Alliance in 2016, "Data Leakage" ranked first [1]. At the same time, due to system vulnerabilities, human leakage, server overload, etc., cloud platform data leakage security events happened frequently[2]. Data security has become a key factor that restricts the promotion and application of cloud storage.

Research on cloud storage security issues mainly focuses on data encryption and storage[3][4], ciphertext access control[5][6], and ciphertext search[7]-[10]. This paper mainly studies the secure storage of user-differentiated data, and proposes a multi-level security task scheduling scheme that comprehensively considers the data security level, user service level, and task waiting time. The scheduling program runs on a heterogeneous multi-core processor, on which data is encrypted before it is transmitted to the cloud storage server.

Related Research

Different user roles and different natures of data lead to different values and sensitivities of the data; even for the same user, the value and sensitivity of the data they own is also different [11]. In order to ensure the security of data, a unified and indiscriminate encryption storage method is currently used, which causes the waste of computing resources and time and fails to ensure high security requirements. Therefore, the storage of data must be balanced between security requirements and performance requirements [12].

The cryptographic algorithm relies on the algorithm itself and the key to achieve different security strengths. Since the algorithm is generally not confidential or even completely public, the security of data depends on the security of the key. In addition to the physical security of the key, the length of the key is the key to security. For a given encryption algorithm, the longer the key, the higher the key strength, and the harder to crack the ciphertext[13][14].

Fine-grained access control based on user classification is implemented in literatures [15] and [16]. In [17], the authors divide the data into different security levels for encryption according to the user's privacy requirements and security level definitions. They considered only different encryption algorithms for hierarchical protection of data, but not the hierarchical protection of files by key strength.

In [18]-[20], the author designed a real-time task scheduler framework to dynamically adjust the security policy of scheduled tasks according to the system security level to achieve the optimal balance of security and schedulability. A task mapping scheduling algorithm for security perception and energy awareness is designed in [21], and a security scheduling method based on user level or SLA to limit the user's resource application is presented in [22][23]. Although these documents all take into consideration the security requirements of user tasks, none of them has designed a differentiated security requirement for user data.

Aiming at the above problems, we propose a task priority-based multi-level security task scheduling scheme for heterogeneous multi-core processors in this paper. The scheme adopts the idea of multi-level security and defines the security level according to the value, privacy, and sensitivity of the file. It meets the differentiated security requirements of user data by choosing the right encryption algorithm and key length to implement differentiated encryption. At the same time,

according to the user's service level and task waiting time in the usage environment, the priority of tasks is defined to determine the sequence of data to be encrypted, and improve the system's computing performance.

Priority-based Multi-level Security Task Scheduling Scheme

The application scenario of the solution in this paper is shown in Fig.1. All terminal users in a LAN share a cryptosystem and upload the data to the cloud storage server after encrypting the data locally.

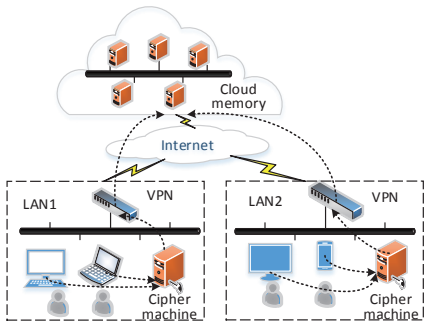

Fig.1. The application scenario

Clients can use a variety of devices such as PCs, tablets, and mobile phones to perform data escrow operations. Cipher machines encrypt data of local users. To achieve different levels of security, block ciphers of 3DES, AES, and SM4 are implemented in this paper. The overall structure of the cryptosystem is shown in Fig.2.

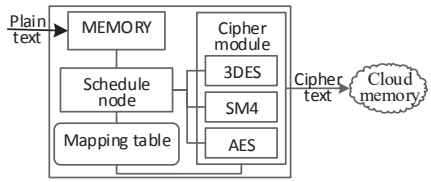

Fig.2. Cipher machine structure

A. Data Security Level and Key Length Mapping

A.1. Data Security Classification

Cloud users need to strictly classify their data according to national standards and relevant regulations of organization or their own needs. According to the degree of importance and sensitivity protection requirements of the user data, we divide it into four security levels based on its type, as shown in Table I.

TABLE I
DATA SECURITY LEVEL CLASSIFICATION STANDARD

Security Level	Security Description	Application Scenario
1	Public	Publicly available documents, videos, etc.
2	Low security level, privacy and security requirements are not high.	E-mail, company policies and standards, etc.
3	Medium security level, privacy security requirements medium.	Intellectual property documents, financial information, etc.
4	High security level, high privacy and security requirements.	Personal identification information, medical records, etc.

The security level is contained in the attribute information of the data. Data attribute Q_i includes the user of the data, the user service level, the security level, the data size, the algorithm type, and the creation time. The user service level is determined by the cloud service provider according to the service quality charging standard.

$$Q_i = \{User_i, Prior_i, level_i, length_i, type_i, creat_i\} \quad (1)$$

A.2. Key Strength Level

Key strength is determined by the encryption algorithm and its length. According to the correspondence between the key length and the key strength of the encryption algorithm, the key strength is divided into 4 levels, as shown is Table II.

TABLE II
SECURITY LEVEL AND KEY LENGTH MAPPING

Cipher Algorithm Properties			Key Strength Level
Cipher	*Key Length*	*Key Strength*	
3-DES	112	80~112	1
	168	112	2
SM4	128	128	3
AES	128	128	
	192	192	4
	256	256	

The key strength level is included in the attribute information of the algorithm. The attribute Alg_i of the cryptographic algorithm includes the cryptographic algorithm, the key length, and the key strength level. It is expressed as:

$$Alg_i = \{Enc_i, size_i, S_{level_i}\} \quad (2)$$

A.3. Data Security Level and Key Length Mapping

In this paper, block ciphers are used to ensure the security efficiency while ensuring the efficiency of encryption. A mapping relationship is established based on the data security level and the key length that implements the key strength level. The specific steps for mapping data security levels and key lengths are as follows:

Step1: Determine the data security level $level_i$ according to the importance and sensitivity of data d_i to be encrypted.

Step2: Determine the key length. According to $level_i$, the key

strength level S_{level_i} corresponding to it is determined. The encryption algorithm Enc_i and the key length $size_i$ are determined according to the algorithm type $type_i$ and S_{level_i}.

Step3: Generate an encryption key. According to Enc_i and $size_i$, key_i with the length of $size_i$ is generated.

Step4: Data encryption. key_i is used to encrypt the data to obtain ciphertext. Encryption can be achieved through hardware encryption, software encryption, and network encryption. Compared with software encryption, hardware encryption has advantages such as fast encryption speed and good encryption performance. This paper uses hardware encryption to ensure task security.

B. Priority-based Task Scheduling Algorithm

Based on the priority task scheduling algorithm block diagram is shown in Fig.3.

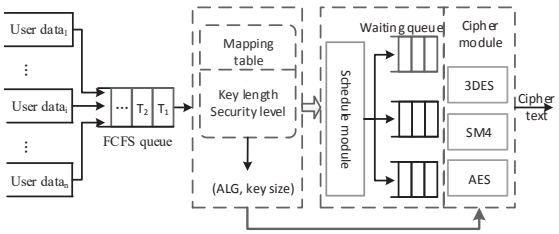

Fig.3. Priority-based task scheduling algorithm

1. Calculation priority. The task priority is determined by the user service level and the task waiting time. The priority of the *i*'th task $Task_i(Q_i)$ is defined as:

$$\begin{cases} Priority_i = \alpha \cdot Prior_i + \beta \cdot Wait_i \\ \alpha + \beta = 1 \end{cases} \quad (3)$$

Where, $Prior_i$ indicates the user service level of the task, $Wait_i$ indicates the waiting time of the task. $Priority_i$ can guarantee the service quality of users at different levels, and ensure the long waiting tasks can be processed in a timely manner.

2. Define the waiting queue. According to the type of encryption algorithm, this paper defines four waiting queues. The scheduling module dispatches the data to the corresponding waiting queue according to the algorithm requirements and waits for the encryption module to perform encryption processing. Tasks in the same waiting queue have priority, but no priority difference between the waiting queues.

TABLE III
TASK PRIORITY

task	$Wait_i$	$Prior_i$	α	β	$Priority_i$
$Task_1$	2	4	0.5	0.5	3
$Task_2$	3	1			2
$Task_3$	4	3			3.5
$Task_4$	1	2			1.5

The priority of tasks in the same waiting queue is calculated according to (3). Assume the waiting queue of 3DES encryption module has four tasks, as shown in Table III. Then the scheduling order of tasks is $Task_3, Task_1, Task_2, Task_4$.

Simulation and analysis

To verify the performance of the proposed multi-level security task scheduling algorithm, simulation experiments are carried out based on open-source cloud computing simulation CloudSim[24]. The task parameter settings are shown in Table IV.

TABLE IV
TASK PARAMETER SETTINGS

task parameter	discription	value
cloudletNum	task numbers	[0,1000]
id	task id	[0,1000]
$length_i$	task length	[100,300]
$Wait_i$	waiting time	$[0,+\infty]$
$Prior_i$	user service level	[1,4]
α	service level factor	[0,1]
β	waiting time factor	$\alpha+\beta=1$

Experiment 1. Comparing the time performance of the RR algorithm[25], greedy algorithm, and our algorithm. The number of task sets is 50, 100, 150, 200, respectively; $\alpha = 0.3, \beta = 0.7$. Fig.4 compares the task set completion time; Fig.5 compares the average waiting time of the scheduling algorithm.

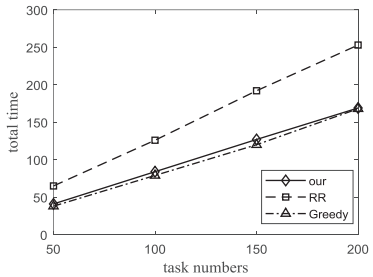

Fig.4. Comparison of task completion time

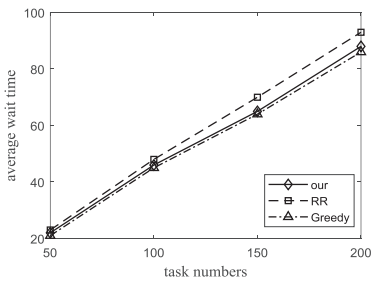

Fig.5. Comparison of average waiting time

From Fig.4 and Fig.5, we can conclude that the time

performance of our algorithm is better than the RR algorithm, and similar with the greedy algorithm. But because the task is scheduled according to the priority, the user experience is different. The number of tasks is set to 100, the sliding window size is 20. The execution result of the task set is shown in Fig.6.

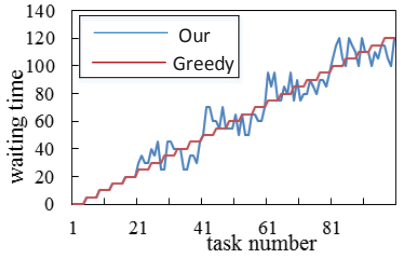

Fig.6. Comparison of task scheduling sequence

Different from the greedy algorithm scheduling according to the task number, the sequence of our schedule is out of order. This is because the scheduling algorithm considers the two factors of the service level and task waiting time. It is more suitable for flexible task scheduling in the cloud computing environment.

Experiment 2. Effect of encryption node processing performance on algorithm performance. The number of task sets is 50, 100, 150, 200. Speed1 indicates that the processing time of one block of the four encryption nodes is 200, speed2 is 200, 200, 300, and 300 respectively, speed3 is 200, 300, 400, 500 respectively. The experimental results are shown in Fig.7. It can be concluded that with a fixed number of tasks, the completion time decreases linearly as the performance of the encryption node increases.

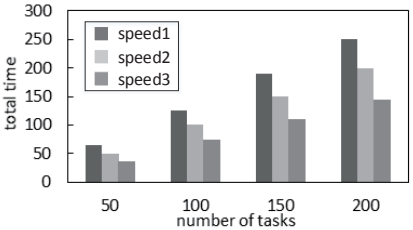

Fig.7. Relationship between task completion time and node performance

Conclusion

A multi-level security task scheduling scheme based on task priority is proposed in this paper. By defining the mapping relationship between the data security level and the key strengths of different encryption algorithms, the scheme realizes multi-level security encryption of data. The task priority is determined by the user service level and the task waiting time. Based on the task scheduling of this priority scheduling, more reasonable user services can be achieved and a good user experience can be obtained. The simulation results show that the scheduling algorithm is better than the RR scheduling algorithm and close to the greedy algorithm. By adjusting the weight coefficient, the priority of task scheduling can be flexibly adjusted.

Acknowledgment

This work is supported by the National Key Research Program of China (No. 2017YFB0801803).

References

[1] 2016 Data Breach Investigations Report[EB/OL] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.
[2] http://netsecurity.51cto.com/art/201603/507516.htm.
[3] S. Rajeswari and R. Kalaiselvi, "Survey of data and storage security in cloud computing," 2017 IEEE International Conference on Circuits and Systems (ICCS), Thiruvananthapuram, 2017, pp. 76-81.
[4] X. Yin, Z. Liu, Y. S. Lee and H. J. Lee, "PKI-based cryptography for secure cloud data storage using ECC," 2014 International Conference on Information and Communication Technology Convergence (ICTC), Busan, 2014, pp. 194-199.
[5] J. Chen and H. Ma, "Efficient decentralized attribute-based access control for cloud storage with user revocation," 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, 2014, pp. 3782-3787.
[6] K. Riad, "Multi-authority trust access control for cloud storage," 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS), Beijing, 2016, pp. 429-433.
[7] Song D X, Wagner D, Perrig A. Practical Techniques for Searches on Encrypted Data[C]// Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000:44.
[8] S. A. Oli and L. Arockiam, "Confidentiality Technique to Encrypt and Obfuscate Non-Numerical and Numerical Data to Enhance Security in Public Cloud Storage," 2017 World Congress on Computing and Communication Technologies (WCCCT), Tiruchirappalli, 2017, pp. 176-180.
[9] K. Kaushik, V. Varadharajan and R. Nallusamy, "Multi-user Attribute Based Searchable Encryption," 2013 IEEE 14th International Conference on Mobile Data Management, Milan, 2013, pp. 200-205.
[10] Xu Wang, Beizhan Wang and Jing Huang, "Cloud computing and its key techniques," 2011 IEEE International Conference on Computer Science and Automation Engineering, Shanghai, 2011, pp. 404-410.
[11] R. Shuanglin, "Data security policy in the cloud computing," 2012 7th International Conference on Computer Science & Education (ICCSE), Melbourne, VIC, 2012, pp. 222-225.
[12] D. Kumar, D. Kashyap, K. K. Mishra and A. K. Misra, "Security Vs cost: An issue of multi-objective optimization for choosing PGP algorithms," 2010 International Conference on Computer and Communication Technology (ICCCT), Allahabad, Uttar Pradesh, 2010, pp. 532-535.
[13] Yearly Report on Algorithms and Keysizes.2012.http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf
[14] K. S. Nag, H. B. Bhuvaneswari and A. C. Nuthan, "Implementation of advanced encryption Standard-192 bit using multiple keys," National Conference on Challenges in Research & Technology in the Coming Decades (CRT 2013), Ujire, 2013, pp. 1-7.
[15] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// ACM Conference on Computer and Communications Security. ACM, 2006:89-98.
[16] T. Yang, P. Shen, X. Tian and C. Chen, "A Fine-Grained Access Control Scheme for Big Data Based on Classification Attributes," 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), Atlanta, GA, 2017, pp. 238-245.
[17] F. Yahya, R. J. Walters and G. B. Wills, "Protecting data in

personal cloud storage with security classifications," 2015 Science and Information Conference (SAI), London, 2015, pp. 838-843.

[18] K. A. Nuaimi, N. Mohamed, M. A. Nuaimi and J. Al-Jaroodi, "A Survey of Load Balancing in Cloud Computing: Challenges and Algorithms," 2012 Second Symposium on Network Cloud Computing and Applications, London, 2012, pp. 137-142.

[19] E. Meriam and N. Tabbane, "Dynamic Priority Scheduling Protocol Based on Cost in Cloud Computing," 2016 Global Summit on Computer & Information Technology (GSCIT), Sousse, 2016, pp. 15-20.

[20] Bhandari, A. Gupta and D. Das, "A framework for data security and storage in Cloud Computing," 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), New Delhi, 2016, pp. 1-7.

[21] H. Li, H. Zhu, G. Ren, H. Wang, H. Zhang and L. Chen, "Energy-Aware Scheduling of Workflow in Cloud Center with Deadline Constraint," 2016 12th International Conference on Computational Intelligence and Security (CIS), Wuxi, 2016, pp. 415-418.

[22] E. Meriam and N. T. Mediatron, "Multiple QoS priority based scheduling in cloud computing," 2016 International Symposium on Signal, Image, Video and Communications (ISIVC), Tunis, 2016, pp. 276-281.

[23] M. Alrokayan, A. Vahid Dastjerdi and R. Buyya, "SLA-Aware Provisioning and Scheduling of Cloud Resources for Big Data Analytics," 2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, 2014, pp. 1-8.

[24] Calheiros R N, Ranjan R, Beloglazov A, et al. CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms[J]. Software Practice & Experience, 2011, 41(1):23–50.

[25] Li T, Baumberger D, Hahn S . Efficient and scalable multiprocessor fair scheduling using distributed weighted round-robin[C].PPoPP '09 Proceedings of the 14th ACM SIGPLAN symposium on Principles and practice of parallel programming.ACM , 2009:65-74.