Security framework for cloud data storage based on multi-agent system

Hui Zhou*, Shigang Qin

Hunan electrical college of technology, Xiangtan 411101, Hunan, China

Received 1 June 2014, www.cmnt.lv

Abstract

Cloud computing environment involves many aspects, including data, users, technology, resources, transactions, etc. It is necessary to establish effective security technology to ensure cloud computing reliable. Multi-agent system architecture is an effective framework to maintain system security. Therefore, we build a multi-agent architecture for cloud data storage issues. This security framework can bring better confidentiality, availability, accuracy, coordination of the operation of the cloud data for cloud computing. Through the analysis of the safety performance of this framework and operating data test, the effectiveness of cloud data storage security framework had been confirmed.

Keywords: cloud computing, multi-agent system, cloud data storage, security framework

1 Introduction

Nowadays, the cloud computing has been extended to the applications available for the Internet, and these cloud applications use large data centers, cloud data storage and powerful servers to host web applications and network services. With proper network connection and a standard Web browser, any user can access the cloud application. Generally speaking, the cloud is co-founded by multiple computing service providers. Judging from the system constitution, the cloud computing system consists of different types of computers, storage devices, communication equipment and software running on these devices [1].Cloud computing environment involves many aspects, including data, users, technology, resources, transactions, etc, thus, the efficient and safe technologies must be used to maintain its normal operation. The data security of cloud computing is involved in not only the data transmission but also the storing data security and data protection of cloud storage. Server vendors must pay attention to the possible problems and have perfect capabilities for database and file management, especially when there are a lot of cloud users to access the same file on the client [2].

In cloud computing, researches on cloud security are an important branch. Many research institutions are dedicated to the development of cloud security solutions and related standards, and a large number of investigations and experiments have been done [3], which have put forward their own security models based on the characteristics of cloud computing and system architecture. In order to make deployment of cloud security more efficient, there are scholars specialized in the experimental validation of the availability of security access control services. According to the practical experience of cloud services of some companies, Forrester established a statistical model based on service quality assessment to assess the quality of cloud security. He pointed out that the typical cloud security architecture could accommodate the running of at least 5-15 applications at the same time [4]. VPN-Cubed model is a typical cloud security framework. In its mechanism, both the single cloud and the hybrid system composed by multiple clouds can be confined to the infrastructure-based secure border. Vertica arranged a database on the cloud of Amazon EC2 and set up VPN links and firewall protection, which achieves better database security protection performance [5]. From the perspective of data integrity, Zetta built a cloud data storage security system to meet the service requirements. He believes that the integrity of data means the undamaged system and incomplete data, even in a huge cloud or during a long period of service. In order to fully accomplish this integrity, Zetta used six nodes of a redundant array to achieve the hosting service of primary data of cloud. In this paper, to further improve the security performance of cloud data storage, a Multi-Agent-based security framework for cloud computing is proposed.

2 Theoretical basis

2.1 SECURITY INDICATORS OF CLOUD DATA STORAGE

In order to guarantee the security of cloud data storage, the following important attributes should be paid much attention to, including confidentiality, accuracy, availability, and integrity [6].

2.1.1 Confidentiality

In cloud computing, security plays an important role, especially when the organized data is maintained by the

* ***Corresponding author's*** e-mail: 274528006@qq.com

distributed cloud server or cloud data storage. The personal information of users of cloud computing is a prerequisite to protect the confidentiality of their data security. Almost at the beginning of the access, the security function should be started in the security protocol of different layers of cloud data.

2.1.2 Accuracy

For the required security, the cloud data should be saved completely and correctly. Even when the cloud users modify, delete, or add cloud services demand, it is necessary to adopt the correctness criteria of cloud data storage at the same level.

2.1.3 Availability

In cloud computing, availability is one of the most critical information security requirements, for it is the critical factor deciding whether the related cloud services could be established when the delivery of supply and demand is completed between cloud providers. As a kind of important information document, Service Level Agreement highlights the availability of cloud service between the provider of the server and client. Thus, according to information security requirements, the availability would promote safe and efficient cloud computing security framework in a variety of cloud computing deployment and delivery.

2.1.4 Integrity

In cloud computing, the integrity means to ensure the atomicity, consistency, isolation, and durability of cloud computing, which is an important factor to achieve the cloud security.

2.2 ANALYSIS OF CHARACTERISTICS OF MULTIPLE AGENT SYSTEM

In fact, the cloud services, to a large extent, are achieved by the agent in charge of exchange messages in the network. While the quality and safety performance of the whole cloud service also largely depend on the interaction, coordination, responsiveness and learning ability of each service node. The performance of cloud services matches the popular multi-Agent [7].The original meaning of Agent in English is the subject, so each Agent should be a subject with adaptability and ownership with its typical characteristics shown as follows.

2.2.1 Initiative

Agent can perceive the outside world and form a certain decision in accordance with the appropriate information. This is also an important manifestation of its intelligence. In other words, even without the top controller, Agent can also give its own feedback. [8]

2.2.2 Interaction

Each Agent is like an individual in a social system. If it is completely closed or isolated, the long-time and reliable work is not available. Therefore, each Agent has good interactive performance, which enables it to keep in touch with other Agent.

2.2.3 Reactivity

When contacting with the outside world, Agent will show the ability to respond in a timely manner. It is this reactivity that allows multiple Agents to form a dynamic converged system.

2.2.4 Learning ability

Different Agents have different performance, and they can form memory and learning processes when interacting and reacting with other Agents, thus constantly updating their own performance.

Perhaps the capacity of an Agent unit is limited, but when pluralities of Agents form an Agent system, the capacity will be very powerful and enhanced sustainably. When multiple Agents work together and achieve integral connection through good synergy, multi-Agent system and cloud storage, cloud computing and the whole cloud service are very similar. Each Agent unit could solve this kind of problem, or request services from other Agent. Inspired by the correspondence between the Multi-Agent system and cloud services, this paper proposed the idea of cloud data storage framework.

3 Cloud data storage framework based on multi-Agent architecture

3.1 OVERALL FRAMEWORK OF CLOUD DATA STORAGE

In order to better achieve security objectives of uploading data and requesting service for users, we established a two-tier cloud security framework. Please see Figure 1.

As can be seen from Figure 1, the proposed cloud security framework can be divided into two layers: one is a cloud data storage layer, and the other is the proxy service layer based on multi-Agent.

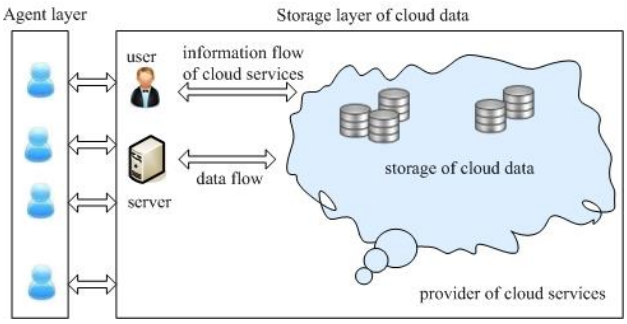

FIGURE 1 Cloud security framework proposed in this paper

3.1.1 Cloud data storage layer

Cloud data storage layer can be determined in two entities. One is cloud service users. They store their data in the cloud and carry out data computing relying on the cloud, and cloud users are divided into individual users and organizations users; the other is the cloud service providers. They are responsible for building and managing distributed cloud storage service with lot of resources and expertise and in charge of cloud computing systems.

3.1.2 The proxy service layer based on multi-agent

The core structure of this layer should include the user interface, which achieves the communication of users and various functional Agent units. Details of its internal structure are described in the following section.

3.2 PROXY SERVICE LAYER BASED ON MULTI-AGENT

We set up five types of Agents in proxy service layer based on multi-Agent: Supplier Agent, confidentiality Agent, correctness Agent, availability Agent, and Integrity Agent. The architecture of the entire multi- Agent service layer is shown in Figure 2. Functions of each Agent and tasks to be finished are shown in the following:

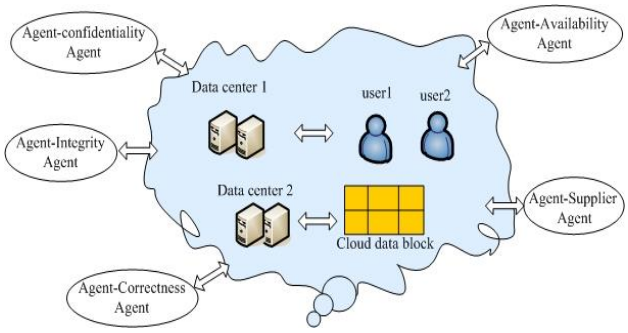

FIGURE 2 Service framework based on multi-agent

3.2.1 Supplier agent

Supplier Agent is connected to cloud service system through interfaces, and it allows cloud users to interact with the secure service environment. Supplier Agent provides the graphic interface for cloud users to facilitate the interaction between system and cloud computing users. The behavior of supplier Agent is under the control of the actual cloud service providers, and its tasks are shown as follows:

[*a*] Provide security services, and send messages to confidentiality Agent, correctness Agent, availability Agent, and Integrity Agent according to the agreement of authorization service level.

[b] Display the specified security policy of supplier Agent and the rest of the system.

[c] Receive safety reports and inform other Agents.

[d] Translate the attacked target.

[c] Monitor related cloud-data memory or activities of specific users.

[d] Create safety report and an alarm.

3.2.2 Confidentiality agent

Confidentiality Agent is primarily responsible for setting confidential security policy of cloud data storage. Especially in the establishment of new access control, this Agent will take charge of authorizing authenticated access control lists. Confidentiality Agent also needs to provide vendor-defined interfaces and data structures for each cloud user. To achieve this goal, it is necessary to set an access control policy of cloud-based data in confidentiality Agent, which is able to define corresponding mathematical formulas for each user's access structure. Confidentiality Security Agent can also notify supplier Agent of technical failure in security reports or alerts.

The formula formed by the data access control policy is defined as security formula. This formula is derived from the multi-Agent architecture of the entire cloud services, rather than the service provider's subjective judgment. Users complete the specific settings of the formula. Security formula is an extra layer of confidentiality used by the system in order to verify the cloud user's login and operating. If you are one of the cloud users, the first time you log in, you will need to register on the system, and fill in a valid e-mail address and enter your security formula. Your security formula will be sent to your e-mail, to prepare for the use of subsequent series of security. It should be noted that the security formula is not your password. Taking logging in as an example, the security formula is applied according to the following steps:

[*a*] Enter your cloud user ID;

[b] Verify your safety formula;

[c] Enter your password to confirm.

What confidentiality Agent guarantees is that even if your password is correct, but your security formula is not, then you will not be able to log on. The architecture of privacy Agent consists of five modules. Please see Figure 3.

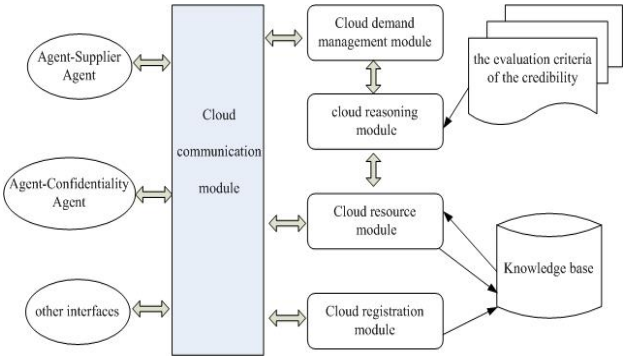

FIGURE 3 Architecture of confidential agent

Cloud communication module is responsible for the information interaction between confidentiality Agent and other Agents, while cloud registration module take charge of the registration function of confidentiality Agent, cloud Demand Management module allows the confidentiality Agent to act as a request dispatch center. Cloud resource management module is in charge of managing the use of cloud resources, and cloud reasoning module is command center of confidential Agent. When demand management module receives a request, it will pass the request to the reasoning module using information from the knowledge base and the evaluation criteria of the credibility by resource module.

3.2.3 Correctness agent

Correctness Agent is responsible for ensuring the correctness of the security policy of cloud data storage. It can perform different block-level operations, and generates correctness guarantee. When the cloud user performs an update operation, deletion, adding, and modification or insert operation with errors occurring, correctness Agent will notify the supplier Agent of sending security reports or alarms. The architecture of Agent correctness consists of four modules. Please see Figure 4.

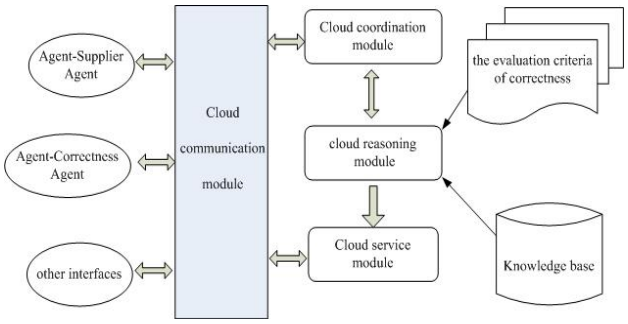

FIGURE 4 Architecture of correctness agent

Cloud Communication Module ensures the information interaction between correctness Agent and supplier Agent. Cloud reasoning module calculates the necessary amount of cloud resources to complete the service at the desired service level agreements, which ensures the implementation of correctness by using the information gained from the knowledge base and the evaluation criteria of the correctness. When the cloud users perform an updating, deleting, appending, and inserting operation, the cloud service module carries out the block-level encryption and decryption operations. Cloud coordination module controls a series of coordination mechanisms, shown as follows:

[*a*] If the data is updated, perform data encryption.

[b] If the data is deleted, perform data encryption.

[c] If the data is appended, perform data encryption.

[d] If the data is inserted, perform data encryption.

Cloud coordination module also sets corresponding priority levels for updating, deleting, adding, and inserting, which is respectively 00,01,10, and 11.

3.2.4 Availability agent

Availability Agent is responsible for the availability security policy of cloud data storage. It maintains contact with supplier Agent through document distribution and document retrieval technology, and sends safety reports and alarms. Under the protection of the availability Agent, malicious resources cannot call the cloud resources. Moreover, it can be used for the troubleshooting of each cloud node.

To further enhance the function of availability Agent, we set up prevention of attacks on local cloud and global cloud. Attacks on global cloud will generally be broken down into the cloud nodes, forming a local cloud attack. From the perspective of general cloud security mechanisms, it can only resist the local cloud attacks. We are trying to break the limits of the cloud data storage through availability Agent, developing resistance to local and global cloud attacks. To this end, the risk probability of attacks from the global cloud is set to 1, while that of the local cloud attack is set to a number between (0,1).

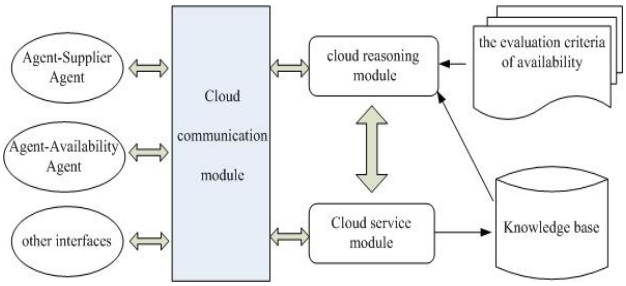

FIGURE 5 Architecture of availability agent

The architecture of availability Agent is shown in Figure 5. As can be seen from Figure 5, availability Agent is generally comprised of three modules. Among them, the cloud communication module is responsible for the interaction between availability Agent and supplier Agent. Cloud service module will distribute redundant data file, which can be rebuilt into the data vector available for the user. Cloud reasoning module combines knowledge base information and the evaluation criteria of availability, which can handle the abnormal behavior of servers as well as collusion attacks from outside the cloud.

3.2.5 Integrity agent

Integrity Agent takes charge of the integrity of the security policy of cloud data storage. It is used to ensure the integrity of the data downloaded from the server by cloud users, or the use of decentralized data for reconstruction. It also regularly sends security reports and alarms to the supplier Agent. Alarm occurs generally in the following circumstances:

[*a*] Human errors during cloud data input.

[b] Errors occur when cloud data is transmitted from one computer to another computer.

[c] Software errors or virus.

[d] Hardware failure, such as the disk crash.

The architecture of Integrity Agent generally comprises three modules. Cloud communication module is responsible for the information interaction between integrity Agent and other Agents. Cloud resource management module is in charge of the manual operation of data backup. Cloud reasoning module checks the reason for data backup failure according to the knowledge base and the evaluation criteria of the integrity. Please see Figure 6.

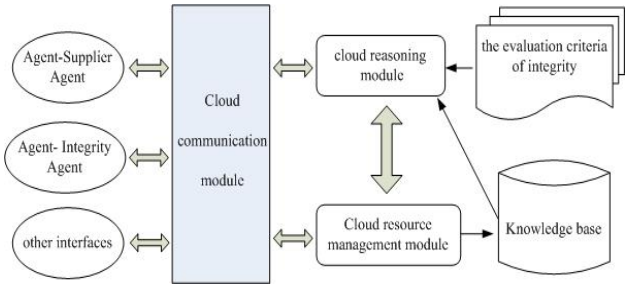

FIGURE 6 Architecture of integrity agent

4 Performance test of cloud security framework

Since the rise of cloud computing is not long, the unified test methods and process of the researches on cloud security have not yet been formed. In addition, the cloud computing platform itself is a service platform, so to assess it often require users' feeling, that is, the subjective evaluation. To test the performance of cloud data storage framework based on multi-Agent, we constructed the corresponding simulation program of cloud service, and invited 15 users to use it in order to evaluate it by the users' comments. To increase the scientific and credibility of the evaluation process, we set the same question items for each user. These items contain the test for cloud security framework and the score for each question is set as five levels 1, 2, 3, 4, 5. The specific items and statistical results of the scores of 15 users are as shown in Table 1.

TABLE 1 Statistic results of question items

Classifying indicators	Indicators of question items	Mean value	Variance
Security	Whether the cloud security system has high security	4.64	0.61
	Whether the cloud services system security settings are perfect	4.81	0.56
	Whether the cloud security response system is timely	4.77	0.46
Confidentiality	Whether the cloud services system has set privacy for the landing system	4.75	0.57
	Whether the cloud service system has set privacy for the data	4.81	0.42
	Whether the cloud service system has set privacy for the task	4.50	0.51
Correctness	Whether the data's receiving and delivering of cloud services system is correct	4.95	0.63
	Whether the task decomposition of cloud service system is correct	4.82	0.54
	The reactivity of the cloud service system at the non-correct handling	4.67	0.43
Availability	Whether the login of cloud services system is convenient	4.83	0.57
	Whether the operation of cloud services system is convenient	4.69	0.52
Integrity	Whether the data's receiving and delivering of cloud services is complete	4.34	0.43
	Whether the execution of cloud services task is complete	4.68	0.35
	Whether the cloud services are capable of reorganizing data and task	4.55	0.45

The statistical results in Table 1 indicate that 15 cloud users speak highly of the cloud security framework based on the multiple Agent.

In order to verify the reliability and credibility of this subjective evaluation, we adopted the reliability and factor analysis commonly used in statistics with the SPSS software as the implementation platform. The basic theory of the reliability analysis of statistical data indicates that when using the same method to conduct repeated measurements for the same data, if we can get close to the consistent results, the statistical data could better reflect the real situation. The reliability analysis at early stage is coefficient a detection method. Generally speaking, the statistical data is reliable when the coefficient a is above 0.5, while it is unreliable when the coefficient a is below 0.35. After reliability analysis, reuse KMO and sphere Pap test to conduct factor analysis. The KMO analysis is reliable when the KMO coefficient is above 0.6 and unreliable when the KMO coefficient is less than 0.5.

Based on this theory, this paper conducted reliability analysis and factor analysis for five classifying indicators. Related results indicate that the coefficient a of classifying indicators of safety assessment - security, confidentiality, correctness, availability, integrity is larger than 0.6, thus confirming that the statistical results in Table 1 has a high credibility. Therefore, it can be applied to factor analysis. The specific results are as shown in Table 2.

TABLE 2 Reliability analysis results

Indicator	Classifying indicators	*a* coefficient	The number of question items
Security assessment	security	0.951	3
	confidentiality		3
	correctness	0.942	3
	availability	0.927	2
	integrity	0.933	3
Overall reliability	0.930		

To conduct further factor analysis, the KMO coefficient was 0.930, so the Pap sphere test is available. The significant probability of Pap sphere test is less than 0.01, thus confirming the reliability of the statistical results. The above statistical analyses has fully validated the reliability and credibility of the question items data of the 15 cloud users, as well as the effectiveness of designed cloud data storage security framework in this paper.

5 Conclusion

The security of cloud data storage is an important condition to ensure the completion of the entire cloud service in high quality. This paper has established the security system framework for cloud data storage with the help of flexibility and convenience, good interaction and strong ability of learning of the multi-Agent system. Throughout cloud security framework, this paper has designed confidentiality Agent architecture, correctness Agent architecture, availability Agent architecture, and integrity Agent architecture. These more specific sub-frames can ensure the security of the entire cloud framework. The application results of the simulation program by the 15 users show that the security framework of cloud data storage designed in the paper has a good safety performance.

Acknowledgments

This work was supported by China Engineering Education Association Annual Project in 2012 (project No.JJX12ZZ015).

References

[1] Yang N, Wang Y, Chen F, et al. 2012 Research on the Identity Authentication Mechanism of Cloud Computing Based on Mobile Agent *Application Research of Computers* **29**(10) 3812-5
[2] Feng D, Zhang M 2011 Study on Cloud computing security *Journal of Software* **22**(1) 71-83
[3] Luo C, Huo S 2011 Identity-based Cross-domain Authentication scheme in pervasive environment *Communications* **32**(9) 111-5
[4] Wang C, Forrester 2009 A close look at cloud computing security Issues *IEEE Transaction on SMC* **12**(9) 544-51
[5] Talib A M, Atan R, Abdullah R, Azmi Murad M A 2011 Mult-agent system architecture oriented Prometheus methodology design to facilitate security of cloud data storage *Journal of Software Engineering* **5**(3) 78-90
[6] Xu B, Guan Q, Chen K 2010 Multi-Agent Coalition Formation Based on Quantum-behaved Particle Swarm Optimization *Journal of Information & Computational Science* **7**(5) 1059-64
[7] Gao Y, Zeng X, Zhou W 2006 Multi-Agent Collaborative Production Management and Its System *Tsinghua University Press: Beijing*
[8] Sadeghi AR, Schneider T, Winandy M 2010 Token-Based cloud computing: Secure outsourcing of data and arbitrary computations with lower latency *Proc. of the 3rd Int'l Conf. on Trust and Trustworthy Computing Springer-Verlag, Berlin* 417-29

Authors

Hui Zhou, 17.03.1972, China

Current position, grades: associate professor at Hunan Electronic College of Technology, China.
University studies: master's degrees in engineering from China University of Geosciences, China in 2013.
Scientific interest: information security and cloud computing

Shigang Qin, 26.01.1979, China

Current position, grades: lecturer at Hunan Electronic College of Technology, China.
University studies: master's degree in computer software and theory from Xiangtan University, China in 2009
Scinetific interest: cloud computing and computer application.