International Journal of Security and Its Applications
Vol. 10, No. 7 (2016) pp.135-146
http://dx.doi.org/10.14257/ijsia.2016.10.7.12

Cloud Computing Education Laboratory Safety Research

Zheng Li

Shandong Women's University,
Ji'nan City, Shandong Province, 250000, China
273684162@qq.com

Abstract

Education laboratory cloud platform has many characteristics, such as access nodes, small regional, and sudden access more, sometimes the need for experimental project needs to transfer the storage and computing resources are not fixed; The safety protection of reason for cloud platform put forward higher requirements. For education laboratory cloud platform carries the characteristics of the business, and the characteristics of the calculation, the security module of the platform, make it effective defense network attack and the risk of systemic paralysis.

Keywords*: Cloud computing; Laboratory; Safety protection*

1. Introduction

With the development of economy, the country more and more money on education, colleges and universities have more money to do their own infrastructure, in terms of infrastructure construction, the laboratory construction is particularly important. In the process of computer laboratory construction, in order to meet the needs of teaching and scientific research, more and more physical server administrators in the process of management found the following questions. (1) low server utilization, for example, a server deployment of a normal website, only such low utilization, caused a serious waste of resources. (2) difficult to manage. With the increase of the number of physical servers, the administrator to know the specific service running on the server, must be documented, and unable to concentrate, operation that increases the difficulty of management. (3) the security and flexibility is difficult to secure. If a server disk is broken, then the data on the server will be lost, the consequence is unimaginable.

Google puts forward the concept of cloud computing in 2006, the company introduced its important cloud computing service, it implements the function of cloud computing infrastructure as a service, and as a public cloud services for individuals and businesses to users. Since then, the IT industry giant have announced to enter the cloud computing, scholars at home and abroad and also makes a deep exploration of cloud computing. Cloud computing based on virtualization, through to the software and hardware virtualization, to provide users with software services, platform service, infrastructure and other services. Established in 2010, Beijing university of technology of cloud computing experiment platform, the platform is based on cloud computing a new generation of high performance computing and data center solutions, is China's first cloud computing examples of successful application in the field of science and education. The experiment platform for schools, businesses, governments, and let the source community, and provide them with high performance computing resources and services considering computer laboratory in colleges and universities are faced with the problem as well as the advantages of cloud computing and services, will be introduced to the cloud computing technology in the computer laboratory construction, using cloud computing technology to build a set of laboratory cloud platform, some of the problems faced in the university computer lab will be improved[1-3].

ISSN: 1738-9976 IJSIA

Through the cloud platform to manage the university laboratory, laboratory faces many problems, will be a good solution. Through the laboratory equipment such as servers, storage and switches together, build a cloud platform, can high efficiency, simple management and use of these physical facilities. Cloud platform for laboratory benefits are as follows: (1) easier to manage. Administrator can through the web or cloud platform client remote management all the resources on the cloud platform, through the platform of the virtual machine name in the right way, you can through the name of information platform of the virtual machine has a preliminary understanding. (2) security. The data on the platform and application security conditions. Cloud platform by installing a firewall switches, connected to the network and the platform of virtual machine is through the VLAN technology to manage and communication, which ensure the safety of the application platform. Platform of data stored in the underlying storage, and the data storage is after the backup, therefore, the data on the platform is safe. (3) reliable and flexible. All applications on the cloud platform exists in storage devices, in the case of a physical server failure, all virtual servers on the physical server automatically migrated to other physical servers, which ensures the system reliability. Can be generated in advance on the platform of virtual machine templates, when a student or a teacher need to directly according to the template to generate the corresponding virtual machine, it embodies the flexibility of the platform. (4) convenient, efficient, to each according to his need. When the user want the virtual machine, only need to apply online, fill in the specific configuration of the server, the administrator after approval, the platform will automatically generate the corresponding virtual machine, it is convenient for the user, also facilitate the administrator.

2. Related Works

2.1. The Basic Theory of Cloud Computing

Since 2006, proposed that the concept of cloud computing, the IT industry has a huge response. Combined with IT technology and Internet technology, cloud computing is to achieve the large-scale computing and storage capacity, is an entirely new and advanced information technology. Its goal is to put the "computing power" as a kind of public infrastructure, organization of very large scale computing resources, software and hardware for the user to provide comprehensive and convenient public services, meet the social and individual's need for information service, like power supply, water supply, the financial system to provide public services. Grid computing, distributed computing, utility computing, virtualization and parallel computing and traditional computing technologies such as a product of the integration of network technology development. This solution simple and efficient, can provide on-demand variable computing resources, meet the users demand of diversification, by individual users and the vast majority of enterprises.

At present, there are many different kinds of definition of cloud computing, has not formed the industry generally accepted standards. The definition of the American national standards institute of technology of cloud computing is more accurate and comprehensive, is accepted by many people.IT is this definition of cloud computing, the user can through the network access to a Shared resource pool, and can be convenient, according to the need to obtain the needed resources, able to quickly deploy cloud users demand, and the management of the minimum cost, service providers can also be as low as possible intervention, is a new type of IT running mode. There are 3 basic characteristics of cloud computing are:

(1) On-demand self-service, when users need to change the calculation ability, can configure itself, without the need for interactions with service personnel of the service providers, such as network storage and server time.

(2) The broadband access, users can use all kinds of terminal, including laptop, mobile phone or PDA, *etc*., through the network to access the cloud system. The user terminal support various fat client platform or thin client platform;

(3) Virtualization resources, computational resources providers will form a unified resource pool, according to the multi-tenant model, according to the needs of users, to dynamically assign multiple users to a different physical resources and virtual resources. Even though the user cannot control cannot know the location of the use of computing resources, but in principle can be used within a certain range to establish position. Computing resources including processing, network bandwidth, the virtual machine, memory, *etc*.

2.2. Security Policy

The transfer of information on the Internet, such as file transfers, or electronic commerce, *etc*., there are more or less security issues, especially on network transmission confidential documents, information security is more important. The Internet is not safe, this is determined by the TCP/IP protocol is not security, therefore, to solve the problem solution is encryption, the encrypted data are obtained by others, before the decryption is unreadable. Data encryption is the core of all the data security. The purpose of network encryption is to protect important information by hackers to intercept or tampered with. New to this and the cloud computing service mode is relying on the Internet, so the cloud user data security transmission requires encryption. Encryption technology, there are two different cryptography symmetric key cryptosystem and public key cryptosystems[4-6].

(a) Symmetric cryptographic algorithm of DES

DES design core idea is: let all the secret lies the key. DES is a grouping encryption algorithm, encryption, with 64 bits for the group unit, the first clear group; Then encrypts each grouping, generate a set of cipher text information, each group of cipher text information is still 64 bits; Final connection between groups ciphertext the encrypted information. The encryption key length is 64 bits, which is used for parity with 8 bits, actually only 56 bit key length.

DES algorithm three stages after the handling of plaintext, (1) replacement IP, according to the bit rearrange each 64 bit block clear, do not use the key here.(2) in the cycle of 16 times associated with key encryption arithmetic, a process that includes both displacement and replacement.(3) inverse initial permutation.

(b) The MD5 Hash algorithm

The MD5 algorithm of arbitrary length of the input value after processing to produce output value of 128.First extended information step is: first of all in 1 filling the information, then use 0 fill other, until the condition is met, no longer use 0 filled information. Before then, the extension of message length with a 64 - bit binary number, said and put it attached after the extension information. Information after such transformation, byte length 512 integer times.

MD5 is A, B, C, D, four 32-bit integer called link variable parameters, their initial values are: A = 01234567, B = 89abcdef, C = fedcba98, D = 76543210.When the four link variables was set up after that, will be four rounds of the main loop operation, each round of cycle number is determined by the number of group information.

First link variable copy, copy A to the AA, copied to BB, B C is copied to the CC, D is copied to the DD. Then began to 4 wheel cycle of operations, each round of cycle operation is essentially the same. Round 1 to 16 times, each operation should be A nonlinear function operation, its operand is A, B, C and D three of the four link variables, and then combined with the text of A constant and A child groups, namely the fourth variable. Recycling mobile S results are then to the left, and add any link variables.

Finally use the results to replace any links to a variable. After the completion of all of these will be A, B, C, D respectively with AA, BB, CC, DD. Continue to execute algorithm dealing with the next packet data, the final output is four link variable cascade.

3. Cloud Computing Security Analysis

3.1. Cloud Computing Security Risks

Although cloud computing service provider has repeatedly said the services it provides are safe, and a third party on the consultation and investigation, but in recent years, frequent outbreaks of security incidents show that the cloud computing service is not mature enough, lack of user trust completely. To analyze the security problem of cloud computing, and summarized into the following two categories: strategic management risk, technology risk.

(a) Strategy to manage risk

Without effective management to the safe operation of cloud computing, loopholes in management rules will result in cloud computing security failure. To reduce or avoid risk problems of strategy and organization management can better guarantee the security of cloud computing services. Cloud computing is faced with the risk management:

(1) lock the user cannot migrate data/services to other cloud providers, or moved back to the local.

(2) the risk of lost: due to cloud providers will all or part of the service outsourcing to a third party, make its services cannot reach agreement security level and the introduction of risk.

(3) the compliance challenges: because of the cloud provider can't provide effective proof to illustrate its services to comply with the relevant provisions, and cloud providers do not allow the user to the audit, and part of the service can't meet the compliance requirements.

(4) due to the activities of other users in the multi-tenant lose business reputation: due to the malicious activities of the other users in the multi-tenant innocent users affected, such as malicious attacks, including the IP address of the attacker and the innocent is blocked.

(5) the cloud service termination or failure: because cloud provider bankruptcy or stop providing services in the short term, the cloud user business suffered serious impact.

(b) Technical risk

In addition to the risk management, cloud computing is also facing technical risk, through the analysis, summed up a cloud computing are faced with the risk of the following technical problems.

(1) resource depletion: because of the cloud provider itself does not provide adequate resources, lack of effective resource prediction mechanism, or resource utilization model is not accurate, make public resources cannot be reasonable allocation and use, will influence the availability of services, and bring economic and reputation losses, *etc*. Also, if you have too much resources, can not effectively management and utilization will bring economic losses.

(2) the isolation failure: because of the cloud computing power, storage capacity and network by multiple users to share, isolate the fault will result in the cloud storage, memory, routing isolation mechanism of failure; Eventually making users and providers lost valuable or sensitive data, service and reputation, *etc*.

(3) cloud internal malicious people: internal staff to senior privilege abuse, will all of the cloud data confidentiality, integrity, and availability, all cloud services, as well as the serious influence company's reputation and customer trust. With the increase of cloud services usage, cloud providers internal employees appear group will also increase the chance of crime, and the phenomenon has been confirmed in the financial services industry.

(4) management interface: for cloud providers to provide services and resources, the user can only be accessed through the Internet or other indirect method, thus the defects of remote access and the browser will introduce security risks.

(5) the transmission of data interception: cloud computing environment is a kind of distributed architecture, and compared with the traditional architecture have more data transmission path, must ensure the safety of the transmission process, in order to avoid sniffing and replay attack and threat.

(6) data reveal that: due to the defect of communication encryption or application vulnerabilities and other factors, makes the data from local or downloaded from the cloud to uploaded to the cloud in the process of the local cause leakage[7-9].

3.3. Cloud Computing Related Security Technology

With cloud computing security architecture related security technology is a part of the divisible, including encryption, access control technology, data integrity, data isolation disaster tolerance. Only guarantee the correct implementation of the safety technology, cloud computing to the safe operation.

(1) encryption technology; Encryption technology can provide communications business flow with confidentiality already, also can offer the user data confidentiality, and it also can provide other mechanisms with added. Cloud on the front end, the client can use SSL encryption technology to guard against false websites, such as phishing fraud, theft, *etc*. In the back-end can also through an encrypted to prevent hackers and privileged users of data theft and tampering.

(2) access control technology; Access control technology including login security and access control technology. For secure login, still no complete solution, the user can through own security to protect against it, such as installing anti-virus software, such as using USBKey certification after login. For access control, on the one hand, should prevent access to cross-border problems caused by the system vulnerabilities, system maintenance personnel access strategy should be paid attention to on the other hand, can be used by the system management account, password, permission. The confidential information stored in the database are all made of ciphertext save, even if also can't get the original system management personnel, key can be held by business users.

(3) data integrity test; After the use of cloud computing, data transmission performance will become the bottleneck of a possible, if applied across the border from the cloud, so this will make work more complex data transmission. Using data integrity inspection technology can prevent to a great extent in the process of transmission delay, packet loss, error problem, guaranteeing that the integrity of the data.

(4) data isolation; For data security risks of mutual interference, can use data isolation technique, and with the web server, run the server, the business system server and domain name is completely isolated, to reduce the single point of attack. Using different database application system data or data table stores, between different application data security. Data between enterprise completely isolated from each other, effectively avoid penetration data between enterprises.

4. Cloud Computing Research Data Security Module

Based on build cloud computing platform used in the experiment, the process of data transmission security problems of the analysis, design and implementation of cloud computing data security transmission system, ensure the safety of the user data in the process of transmission and integrity.

4.1. The Construction of the Cloud Computing Platform

Cloud computing system is a large and complex system, not a single person can be done. So the design and implementation of cloud computing systems just have some basic characteristics of cloud computing, such as the integration of computing and storage, calculation of migration to the storage, file distributed storage, parallel computing. Cloud computing devices can be divided into three roles: the primary server node, piece of server and client. The primary server and block the server cluster constitutes the server side of cloud computing, the client through the API calls to achieve access to the cloud computing system. The main server node does not directly storing user data, only responsible for the management of child nodes and users. Cloud users send control commands to the main server requests, and from the main server nodes access to user file information is stored, by returning the node information, connect the child nodes, to child nodes stored command, realize distributed storage of files. If to achieve computing functions, by the user files stored information for file storage of all child nodes, and start the nodes at the same time, parallel computing, in each child node to complete the function of calculation, the results back to the client, computing to store transfer[10-11].

(1) the client. Cloud computing client can be a variety of equipment, desktop computers, laptops and mobile phones, *etc*. The client's main work mode from the main server node system information, according to this information to connect directly with all the child nodes, file operation and computing task. When the client communicate with cloud computing system, important data may be stolen by the outside world. At this point must be encrypted transmission of important data. And session key must also be sent to the cloud server, which between the client and the cloud servers will establish a mutual understanding of the secret channel. However, this will cause another problem - how key distribution, direct transmission in the transmission channel, if the session key may be hacked, user information will be leaked. So, also need to be encrypted session key, in this paper, the use of asymmetric encryption technology to encrypt the session key. In this way, even if the hacker had intercepted the session key, but unable to decrypt, also can't use, make sure the safety of user information. In addition, in order to ensure that information has not been doctored, in cloud computing server receives the user message, must carry on the message validation.

(2) the main server nodes. Master server nodes in this system only communicate with the client, the child node information in the storage system and user registration information, and according to the user's storage requirements, look for free child nodes, allocation of resources for the user to the server. In the main server nodes will save two system information file: root. Dat and node. Dat.Root. Dat file save user name and the user file system where the IP address of the child nodes, the userInfo data structure is used to describe the;Node. Dat file all the child nodes of the cloud computing system's IP address, the total space and space available information, such as distribution server resource usage for the user. As shown in Figure 1 for cloud computing resource allocation sequence diagram.

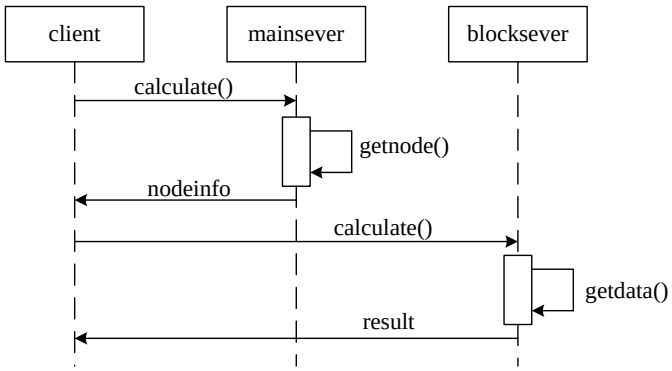

Figure 1. Cloud Computing Resources Allocation Sequence Diagram

The client want to apply to the cloud computing services, you must first and primary server and the main server in accordance with the relevant system information, and according to the largest remaining space priority strategy distribution computing nodes; Then send the client the compute nodes information, thus directly by the client according to node information and compute nodes connection is established, the realization of computing services, and the results back to the client.

(3) block server child nodes. Server is composed of multiple child node, is a compute cluster, its role is more a cloud computing nodes, and the results will be sent back to the user. In addition, still have storage capabilities, to store user data distributed in more than one compute nodes. As a result, cloud computing the client does not need too. Client application using the user name, file name, block number and the IP address of the data block information file information, any data blocks can be uniquely determined the location and filename, the client at the same time send command to start the computation to each child nodes, each node on the read data block local files, and carries on the calculation, calculation with the coma back to the client a summary to get the final result. The calculation process without moving any data for the processing of data in storage data block node to complete, system according to the client's instructions, will be completed calculating migrated to nodes in distributed, greatly improving the calculation efficiency, avoid the data in the network of itinerant efficiency caused by the fall, for huge amounts of data, the effect of this practice is quite obvious[12-15].

4.2. Key Generation and Information Encryption Module

Information encryption can ensure the safety of users of cloud data transmission, so the key generation and information encryption module is designed in this paper the cloud data security transmission system is a key module, the program execution process is shown in Figure 2.

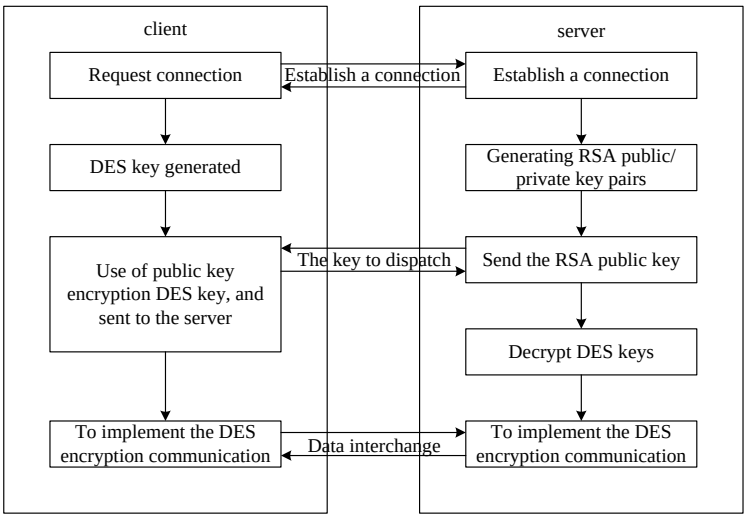

Figure 2. Information Encryption Module Program Flow Chart

When the client ask cloud computing server for cloud computing, cloud computing node first generates a RSA public/private key pairs, and the RSA public key is sent to the client.At this point, the client has to generate and maintain his own DES keys, and use the cloud computing server terminal node forwards the RSA public-key encryption DES keys, and put the encrypted DES key is sent to the server terminal nodes. Terminal and server nodes with their RSA private key to decrypt the client sends over DES keys, since then, both the client and server to establish a mutual understanding of the secret passage, and use the DES encrypted data, for data exchange. So even if the user data to be intercepted during transmission, because no DES key, also don't have access to user raw data; Further even if DES key also be intercepted, but after the RSA public key encryption, and decryption key RSA private key is stored in the cloud computing server side, silent interceptor cannot decrypt DES keys, so double encryption to ensure the safety of the user data transmission.

4.3. The Message Identification Module

Although through information encryption technology to ensure the user data is not leaked, but cannot guarantee that user data will not be altered. Cloud computing security data transmission, therefore, cannot leave the message identification technology, as shown in Figure 3 for cloud computing data security transmission system identification module of the working principle of news.

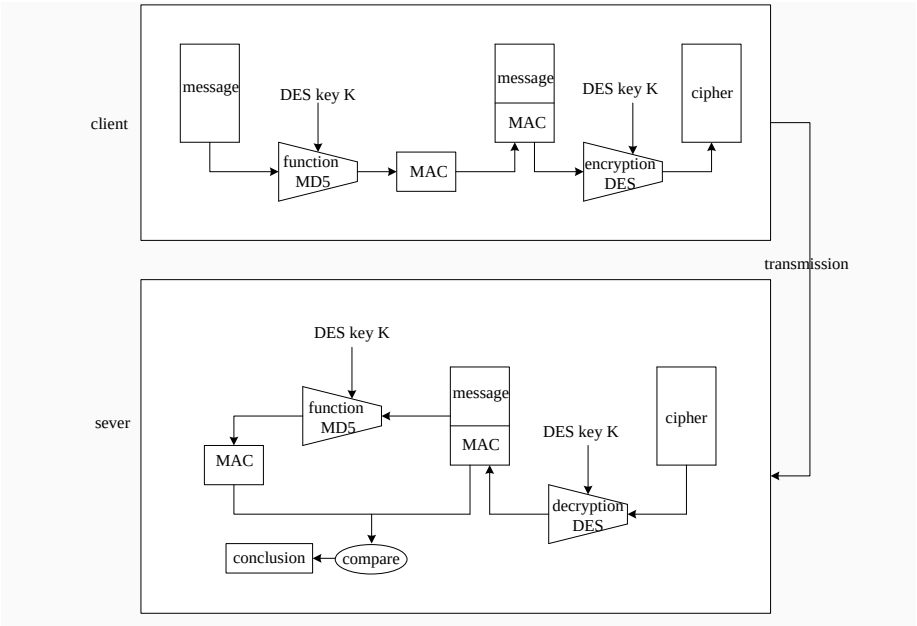

Figure 3. The Working Principle of Message Identification Module

4.3. Cloud Computing Data Security Transmission Process Design

Cloud computing data transmission through the network, the network is an open environment, there is a certain risk. In this paper, design of cloud computing security transmission system USES the double encryption technology, not only ensure the safety of user information, effective transmission, and ensure the safety of key distribution. At the same time using the message identification technology to ensure the integrity of the user data, to prevent the user data has been tampered with. This summary on the overall design of cloud computing data security transmission process, as shown in Figure 4, cloud computing data security transmission system sequence diagram is given.

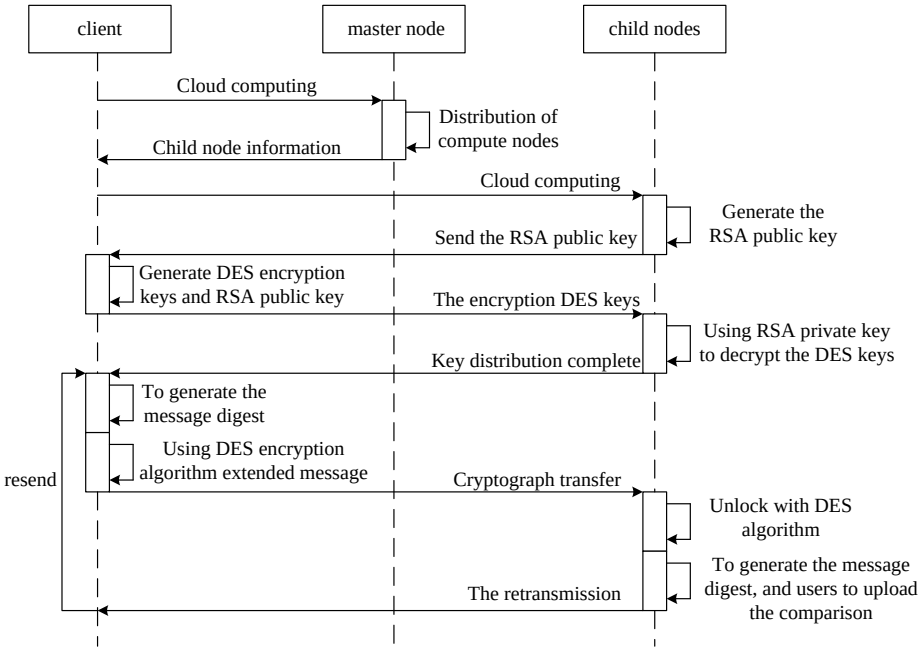

Figure 4. Cloud Computing Data Security Transmission System Sequence Diagram

As shown, when the client sends a message to the cloud server, first calculate the summary of the message, message authenticated code. Client application first with the help of a hash function, here we use the MD5 algorithm, combining DES keys, to generate the message digest MAC; Then the attached behind the information, and use the DES algorithm encryption cipher text, together to send to the cloud server. Cloud server receives the user sends to the news of the cipher text, using DES key decryption, recover the message and the; Then use the same hash algorithm, here we use the MD5 algorithm to calculate the information of the MAC, and compared with forwards the MAC, to identify the message, such as agreement, accepted, or discarded.

5. Conclusion

For cloud computing security problems exist in the process of data transmission in puts forward the strategy, not only ensure the user data is safe and efficient transmission, and ensure the safety of encryption key distribution. Joined the information identification technology at the same time, prevent information being tampered with. Cloud computing general system architecture is analyzed, designed and implemented a cloud computing security module, make the system more secure and practical.

References

[1] Fernando N., Seng W. L. and Rahayu W., "Mobile cloud computing: A survey[J]", Future Generation Computer Systems, vol. 29, no. 1, **(2013)**, pp. 84–106.
[2] Khan A. N., Kiah M. L. M., Khan S. U., "Towards secure mobile cloud computing: A survey[J]", Future Generation Computer Systems, vol. 29, no. 5, **(2013)**, pp. 1278–1299.
[3] Garg S. K., Versteeg S. and Buyya R., "A framework for ranking of cloud computing services[J]", Future Generation Computer Systems, vol. 29, no. 4, **(2013)**, pp. 1012–1023.
[4] Ratten V., "A US-China comparative study of cloud computing adoption behavior: The role of consumer innovativeness, performance expectations and social influence[J]", Journal of Entrepreneurship in Emerging Economies, vol. 6, no. 1, **(2014)**, pp. 53-71.
[5] Xiao Z. and Xiao Y., "Security and Privacy in Cloud Computing[J]", Communications Surveys & Tutorials IEEE, vol. 15, no. 2, **(2013)**, pp. 843-859.
[6] O'Brien J. S. and Julien P. Y., "Laboratory Analysis of Mudflow Properties[J]", Journal of Hydraulic Engineering, vol. 114, no. 8, **(2014)**, pp. 877-887.
[7] Haribhai H. C., Bhigjee A. I. and Bill P. L. A., "SPINAL CORD SCHISTOSOMIASIS: A CLINICAL, LABORATORY AND RADIOLOGICAL STUDY, WITH A NOTE ON HERAPEUTIC ASPECTS[J]", Brain, **(2014)**.
[8] Jonathan D., Christian C. and Bernard C., "Impact of apixaban on routine and specific coagulation assays: a practical laboratory guide.[J]", Thrombosis & Haemostasis, vol. 110, no. 2, **(2013)**, pp. 283-294.
[9] Fang J. J., Zuo K. H. and Zhu D. R., "Safety Protection Technology of WC5E Explosion-proof Vehicle[J]", Mechanical Engineering & Automation, **(2014)**.
[10] Zhao B., Cen W., Zhai F., "Electric Vehicle Charging Pile Control Device with Safety Protection Function[J]", Low Voltage Apparatus, **(2013)**.
[11] Xu G., Ding Y. and Hu L., "Research on Mobile Cloud Computing[J]", Journal of Convergence Information Technology, vol. 8, **(2013)**, pp. 341-348.
[12] Shaha S., Shinde P. and Somatkar S., "Ensuring Data Storage Security in Cloud Computing.[J]", Iosr Journal of Engineering, vol. 13, no. 2, **(2014)**, pp. 95-96.
[13] Chang V., Walters R. J. and Wills G., "The development that leads to the Cloud Computing Business Framework[J]", International Journal of Information Management, vol. 33, no. 3, **(2013)**, pp. 524–538.
[14] Jain R. and Paul S., "Network virtualization and software defined networking for cloud computing: a survey[J]", Communications Magazine IEEE, vol. 51, no. 11, **(2013)**, pp. 24-31.
[15] Kandias M., Virvilis N. and Gritzalis D., "The Insider Threat in Cloud Computing[M]",// Critical Information Infrastructure Security. Springer Berlin Heidelberg, **(2013)**, pp. 93-103.

Author

Zheng Li, won bachelor's degree of Information Management and Information System in Shandong University of Finance in 2005, and master's degree of Engineering in Ji'nan University in 2012. At present, he serves at Shandong Women's University as an experimentalist, whose duty mainly covers modern education technology research and lab administration.