Research and Design of Cryptography Cloud Framework

Sun Lei, Wang Zewu, Zhao Kun, Sun Ruichen, Li Shuai
Zhengzhou Information Science and Technology Institute
Zhengzhou, China 450001
e-mail: zewu0307@foxmail.com

***Abstract*—Since the application mode of cryptography technology currently has different types in the cloud environment, a novel cryptography cloud framework was proposed, due to the non-expandability of cryptography resources. Through researching on the application models of the current encryption technology, the cryptography service demand under the cloud environment and the virtual structure of the cloud cryptography machine, this paper designed the framework of the cryptography cloud framework that provides cryptography services with the cloud computing mode. the design idea of the framework is expounded from two aspects include the function of modules and service flow of cryptography cloud, which resulted in the improvement of the flexibility of the application of cryptography technology in the cloud environment. Through the analysis of system function and management mode, it illustrated the availability and security of cryptography cloud framework. It was proved that cryptography cloud has the characteristics of high-availability in the implementation and experiment, and it can satisfy cryptography service demand in the cloud environment.**

Keywords-cryptography cloud; cloud computing; cloud cryptography service; cryptography resources; virtualization

I. INTRODUCTION

At present, information technology with the rapid development promotes the rhythm and pace of society. With the assistance of characteristics of cloud computing that include high scalability, high reliability and flexibility, more and more application systems migrate to the cloud to deployed, for achieving the goal of centralized management of data and efficient use of resources. Cloud computing technology has been widely used in the information system of industry, finance and government, which greatly facilitates the work and life of people; at the same time, network information has become an important strategic resource, whose security can't be underestimated. To protect security of information data in the network environment, cryptography application mode under the cloud computing environment becomes particularly important. While the traditional cryptography technology is limited to fixed carrier and non-scalable cryptography computing resource, so that it can't satisfy the encryption requirements of massive cloud data [1].

The conception of Crypto as a Service (CaaS) [2] [3] developed the concept of cloud computing from the aspect of information security, it finds a new way for the application of the cryptography technology in the cloud environment, also helps to innovate the new method. According to the report of cloud computing standard [4] published by the NIST in 2011, the security of cloud computing can be divided into 3 parts, which are the security of cloud application, the security of cloud data and the security of cloud hardware with the virtualization. Thereinto, the security of cloud application is mainly about the research on terminal equipment and network equipment supported by trusted technology, also on the reliability and security of outsourcing calculations; the research on cloud data security includes confidentiality, integrity, consistency and reliability of cloud storage data; the major research on the security of cloud hardware with the virtualization are vulnerabilities of hardware facilities in terms of virtualization, security protocols and strategy of virtualized network and security technology of cloud resource pool as well as the upper virtual machine [5]. Cloud cryptography service providers that include Amazon Web Services (AWS), Alibaba Cloud, JN TASS and Sansec have put forward high-available security solutions of the cloud, such as AWS CloudHSM service that is the first one to be achieved commercialization. In addition to that, CloudHSM service mainly provides key management functions for the AWS cloud, and hardware security module (HSM) in which has the function of storage and management of users' private key, and has the characteristics of high-speed calculation and high-level security requirements [6]. Alibaba Cloud launched cloud data encryption service [7] jointed JN TASS, which is to provide credible data security solutions for users that based on hardware cipher machine certified by State Cryptography Administration (SCA). Sansec put forward a series of cloud security solutions from the perspective of infrastructure security, application platform security and network transmission security, all of which have the responsibility of a guarantee to protect security of keys and the credibility of cloud cryptography service.

At the present stage, most of cryptography applications have provided protection of business application information by the cloud cipher machine and other hardware devices. So that, research on cloud cryptography service that is based on facilities with virtualization function is becoming gradually mature, but it still lacks the cryptography service system with cloud computing model to provide cryptography services. Therefore, to improve the flexibility of cryptography service in cloud environment. this paper studied and designed a cryptography cloud (CC) framework, and analyzed its usability and security.

978-1-5386-4301-3/18/$31.00 ©2018 IEEE

II. RELATED APPLICATIONS

Currently, the realization of cloud cryptography service mainly depended on the deployment of cryptography equipment in cloud environment, such as the cloud server with HSM built-in that AWS and HUAWEI had launched, the trusted server that was the innovation of INSPUR and the cloud security solution based on crypto card that was developed by Sansec. Focused on the security of cloud data center, it is the main solution to "three-in-one" cloud security hierarchy include hardware security, system safety and software security, and which is based on security and reliability of the underlying trusted hardware equipment. What's more, using the key with confidentiality and controllability, it could strengthen security protection of the system to provide high security-level hardware encryption service for application data.

Design of cryptography service system has lots of types, which is mainly based on the traditional cipher machine, also it has been unable to meet the requirements of data security under the current cloud computing environment. KOU [8] presented a high-performance cryptography service model, through the design of a unified service interface and the corresponding cryptography sources scheduling algorithm, aiming to achieve unified management for cryptography service resources of different cipher machines. But it is still insufficient in the aspects of security management of keys and performance of cryptography service, such as key security issues and performance isolation problems. Aiming at the security of keys, WANG [9] presented a cryptography service framework based on the third party that key management center. Keys are stored in the third party that is creditable, and access control policy and authentication technology are used to prevent confidential information of users from malicious tampering or pilferage. The illegal user accesses their own key information according to their requirements, but trust of the third party can't be measured objectively, so there are still existing security risks to a certain extent. The wave of trusted server of INSPUR launched a fundamental solution to the trust problem of key management center. From the BIOS to the hardware system of server, and then to the operating system and applications of system, trusted measurement technology makes the basic hardware facilities of key management center credible fundamentally. However, it still couldn't get rid of embezzlement of the internal manager, and to solve which, it needs to strengthen the constraints and management from the angle of policies and regulations [10].

Ciphergraph in cloud environment is applied in the whole cloud service hierarchy that include three layers, IaaS, PaaS and SaaS[11] respectively. And which provides cryptography resources and services for security measures used in the service hierarchy, including all kinds of cryptography algorithms, cryptography application interfaces and cryptography service protocols. AWS CloudHSM services, encryption services of Alibaba Cloud [19] and key management services of HUAWEI all supported by HSM, also, which is used as a key deposit carrier deployed in cloud computing environment. as shown in Figure 1, cryptography service mode.

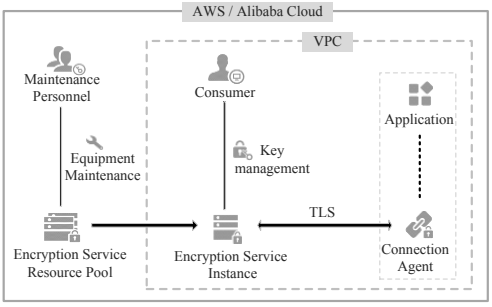

Figure 1. Cryptography service mode

Public cloud is composed of a plurality of virtual private cloud (VPC). The cloud encryption service resource pools are formed by cloud cipher machine cluster that supported virtualization functions. And maintenance personnel are responsible for the maintenance of cloud cipher machine and technical support. Besides, cloud encryption service resource pools connect with VPC through physical network, and provide whom with cryptography service instances. Communications channel between business cloud and cryptography service instances are encrypted by security socket layer (SSL) protocol to meet cryptography service demand of business application. Key management service is the most important part in cloud environment, and to ensure that the encrypted data of consumer is secure, it does not save encryption data key (DEK) that under the plaintext or ciphertext state which encrypted by consumer master key (CMK). CMK is controlled by consumers to ensure that cryptography service instances can securely access DEK of users. Figure 2 is the key management service architecture that is mainstream currently. Consumers can encrypt data by DEK that provided by key management service (KMS) to ensure that critical business data is secure. Thereinto, business data is encrypted by DEK, and DEK is encrypted by CMK that stored in key management center (KMC), besides, CMK is encrypted by root key based on HSM that as the root of trust to ensure that root key can't be stolen from outside of the system, thereby, a complete chain of trust can be structured. In addition, information channel is encrypted by transport layer security (TLS1.2) protocol between HSM and KMS, and which between KMS and business to ensure the reliability of the chain of trust.

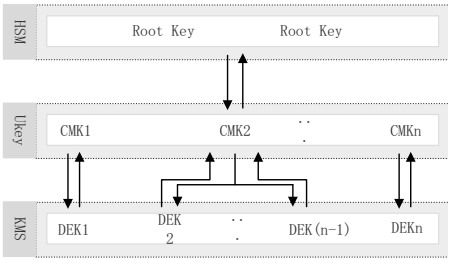

Figure 2. Key management service architecture

The development and application of cloud cryptography services simplified the design and implementation of

cryptography service system, so that the use of ciphergraph in the cloud environment become normalized, and consumers commonly need encryption and decryption operations to hold data [3] [16]. In addition, the management and distribution of keys and credentials can exist as basic security services. Drawing on the characteristics of the current cloud cryptography services, and for the sake of that the cryptography service system become more adapted to cloud computing environment, it is imperative to study the cryptography service system, which needs to be studied a further design with key management function, flexible extension, easy to use, and meeting regulatory compliance requirements.

III. FRAMEWORK

A. Requirement Analysis of Cloud Cryptography Services

As more and more business systems are deployed or migrated to the cloud, the application problem of traditional ciphergraph in the cloud environment are becoming more and more highlighted [17]. However, there are mainly four aspects to expatiate. First, restriction of the relevant cryptography standard and policy; Second, cryptography computing resources could be wasted partly, and maintenance management is difficult; Third, management and use of the key are characterized by decentralization and complexity, and there is the risk of security and management; Fourth, the way that cloud provides keys and cryptography services to consumers is unsafe and untrusted.

Cloud computing has the characteristics of elasticity calculation and dynamic expansion, and it has great flexibility on the supply side of computing resources. The cryptography service system adopting cloud computing mode is easy to meet the requirements about encryption capability aiming at the massive data that is dynamically migrating. Based on the idea of software define cryptography, the cryptography resources are virtualized into a cryptography resources pool by virtualization technology (VT), and which provides consumers with cloud cryptography service based on network according to their needs. What's more, computing ability of the system is elasticity-extendible, to provide cryptography services that can be dynamically scheduled and to manage keys that is unified and efficient. Besides, it can avoid cryptography resources being idle or insufficient.

B. Virtualization Structure of Cloud Encrypt Machine

Cryptography cloud provides consumers with secure and reliable cryptography services. The user-oriented cryptography service provider is Virtual Cipher Machine (VCM). VCM is a complete cipher machine system that is a software-simulated system with functions same as hardware encrypt system, and which runs in a completely isolated environment. Figure 3 shows virtualization structure of cloud cipher machine.

Cloud cipher machine supports hardware virtualization technology, and which transforms the traditional crypto device into a cloud crypto device that supports deployment in cloud. The devices in the underlying hardware system, such as CPU, memory, network device and crypto card, are logically divided into multiple virtual Units, such as vCPU, virtual memory, virtual crypto card (vCC) and so on. KVM manages and organizes cloud cryptography functions using VCM as service carrier. Thereinto, crypto card provides shareable cryptography resources based on single-root I/O virtualization (SR-IOV), and the SR-IOV standard allows efficient sharing of PCIe devices between VCMs, and it can possess I/O performance comparable to that of host machine [11][10]. VCMs are isolated from each other and have completely isolated key systems and spaces. To ensure the absolute security of consumer keys, all cryptography operations are ultimately completed by crypto cards, besides, plaintext keys only appear in hardware.

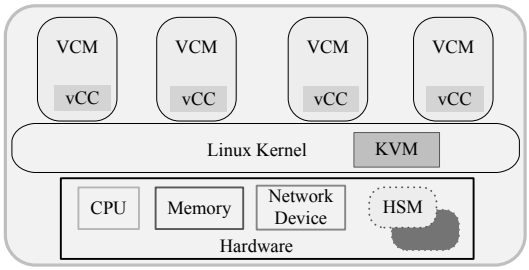

Figure 3. Virtualization structure of cloud cipher machine

C. Design of CC Framework

1) General framework

Cryptography service system in cloud environment that provides cryptography service with cloud computing mode is called CC. And it provides cloud users with three types of cloud cryptography services, there are cryptography components based on network, cryptography middleware, and cryptography application system. The infrastructure of cryptography cloud is a cluster of cloud cipher machines to form a cryptography computing center (CCC). The core of cloud cipher machine is crypto card, and it is better to make full use of its hardware system by virtualization technology. The management of consumer identities, keys and tasks on CC are responsible for the corresponding function modules, and the unified management and monitoring of underlying cryptography equipment are achieved through modular way. Figure 4 is a CC service mode diagram that shows the service structure relationship among consumer terminal, business cloud and CC.

Cryptography cloud is a security service center of cloud computing system for cloud users with a variety of password technology services such as digital signatures, public key cryptography and symmetric encryption technology. Cryptography algorithm is actualized by the way of underlying hardware programming. The management and storage of keys come true by accessing control to trusted root key and strategies that master-slave key authorization. The network communication among modules of the CC is protected by encryption channel with TLS1.2, The communication between service cloud and cryptography cloud adopts the network security transmission strategy based on the idea of software-defined security [12]. CC is characterized by crypto computing capabilities that can

flexibly expand and a variety of cryptography services. CC and ecumenic cloud computing system are based on network computing service model, but CC as a special cloud computing system, needs high-security network measures. Drawing on the concept of feasible region that put forward by Amazon, paper defines the isolation policy of security domain based on service object. And work area of cryptography service that belongs to one consumer can be abstracted as security domain of CC. Besides, based on the idea of software defined network, it provides a secure network isolated area for consumers. It is isolated among secure domains, and the communication channel within them is encrypted by TLS1.2 protocol to send encrypted data.

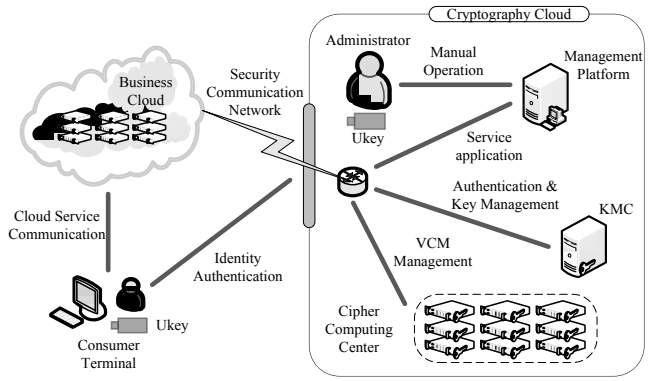

Figure 4. Service mode of Cryptography Cloud

2) Function analysis of modules

Cryptography cloud is divided into three parts, namely management platform of CC, key management center and CCC. Thereinto, the management platform consists of VCM management scheduler, monitor of cloud cipher machine, network manager and authentication module, and the main function of it is operational decision-making, authentication and subnet management; Key management center is composed by certification authority module and keys escrow subsystem, mainly responsible for the authentication to user identity, system management platform and VCM instance, as well as DEK management; CCC is made up primarily of clusters of cloud cipher machines, the virtualization structure of each cloud cipher machine is used as shown in Figure 4, to expand cryptography computing capabilities of CC.

Figure 5 is functional structure diagram, indicating the relationship among sub-modules. VCM management scheduler, monitor of cloud cipher machines and network manager form a scheduling decision ring, and after collecting and processing system information, a schedule and decision about the VCM and related keys will be formed, as well as security isolation strategy between virtual subnets. The authentication module is the authentication agent of certification authority module belongs to key management center. And it transmits authentication request and result of consumers in the management platform of system, meanwhile, it is also responsible for initiating authentication request of the virtual subnet to certification authority module and result feedback. Besides the request information of the authentication agent, certification authority module is also responsible for authorizing VCM instances and related keys of consumers. The main function of key escrow subsystem is to store and distribute encrypted DEK, and adopting trusted technology to ensure integrity and reliability of all keys in the system. VCM is a cryptography service instance, and as a process in user space of operating system of cloud cipher machine of CCC. When certification authority module confirms whose identity, VCM could complete cryptography tasks through invoking the required DEK.

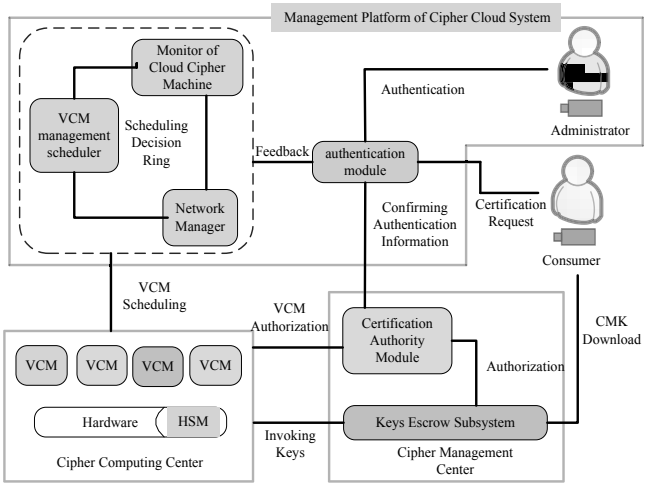

Figure 5. Functional modules of Cryptography Cloud

3) Design of cryptography service flow

Cryptography cloud is divided into piecemeal unit of work region based on the complete security domain that is consumer-oriented, to provide consumers with on-demand cryptography service. In short, cryptography service flow generated by consumer is completed within the corresponding security domain in CC. Figure 6 is a chart named cryptography service flow, illustrating the working mechanism of CC when consumers invoke cryptography service.

The consumer-oriented service processes of CC can be divided into two phases, phase one is the authentication and system services preparation, and phase two is the management and scheduling of cryptography service. The consumer-oriented service processes of CC can be described as follows:

a) When USB key (Ukey) equipped with CMK is inserted into one terminal, it initiates an authentication request to the authentication module;

b) The authentication module forwards authentication information of consumer to certification authority module of key management center. After consumer identity is confirmed correctly, the identity confirmation will be fed back to authentication module.

c) After the authentication module receives confirmation message, it immediately sets mark that ordering encrypted CMK to be downloaded on the terminal and waits for key escrow subsystem to apply for that CMK. Meanwhile, VCM management scheduler is notified to join

VCM of consumer to the dispatch queue list, and inform the network manager to set a security domain for the consumer.

d) The network manager uploads new network deployment information to the monitor module, while VCM management scheduler updates the security domain management strategy according to new monitoring information, and then deploys VCMs in the CCC.

e) When VCM instance is generated and enabled, VCM entity applies for authentication to the certification authority module. And when verifying that the VCM instance has successfully authenticated, the certification authority module sends back the result to the VCM instance and sends key authorization signal to key escrow subsystem.

f) Key escrow subsystem sends CMK download signal to the terminal, only when it is matching with CMK download mark, ciphertext CMK in the Ukey can be downloaded to the key escrow subsystem. And plaintext CMK encrypted by root key is used as the secondary key to encrypt DEK, besides, DEK protected by root key can be obtained.

g) When VCM invokes keys to provide cryptography service for business cloud, VCM instance that authenticated by certification authority module can directly send a key transfer request to key escrow subsystem. And after receiving key transfer feedback, the related DEK would be downloaded through secure communication channel to execute cryptography service.

h) VCM provides the cryptography service, meanwhile, the monitor continuously collects the status information about VCM, cloud cipher machines and network, to help the final decision through making statistics and calculations on the information.

i) VCM management scheduler makes a schedule plan about VCM instances to deploy in CCC according to monitoring information and scheduling strategy.

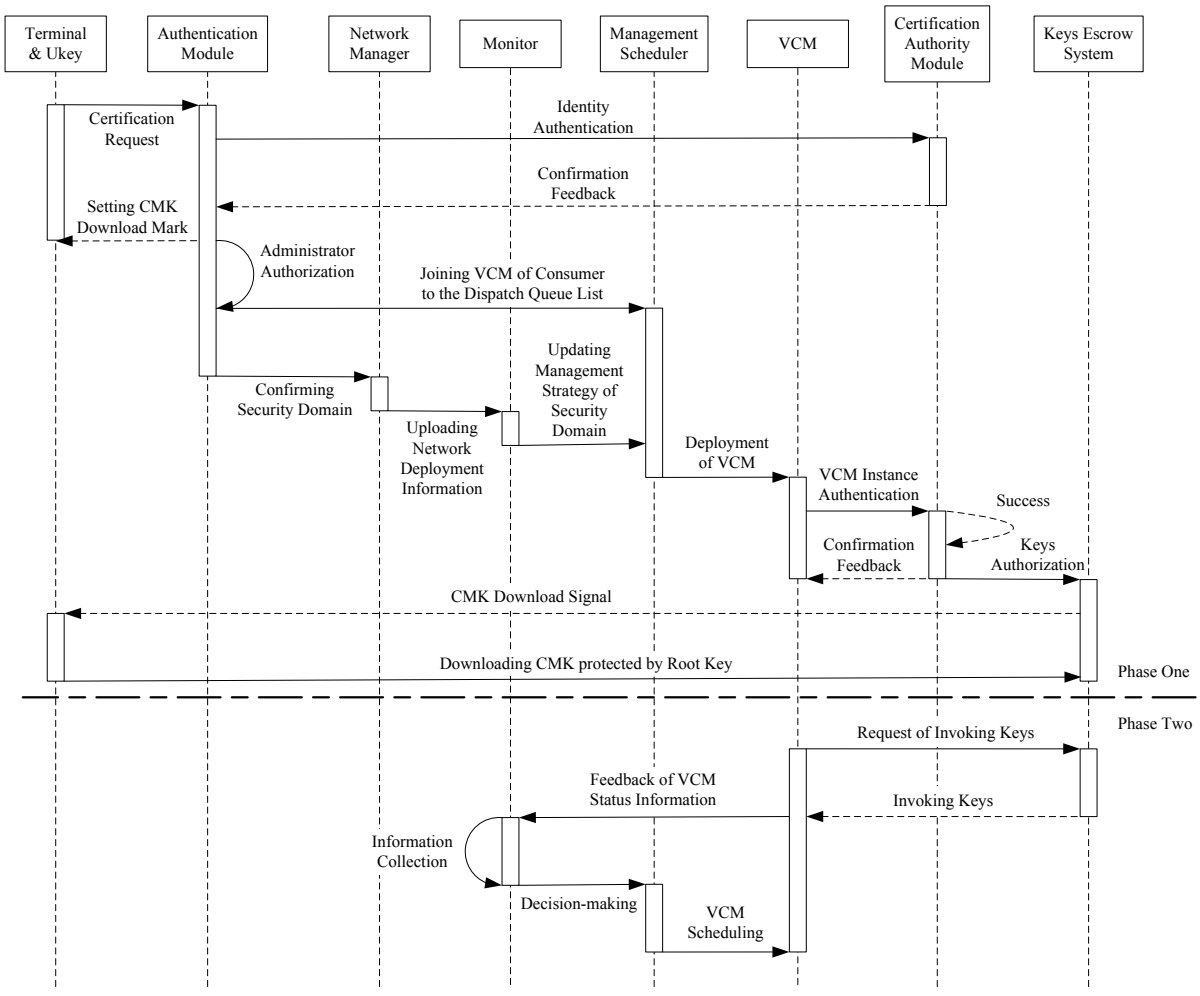

Figure 6. Cryptography service flow

Thereinto, steps from a) to i) of the flow would be phase one, and the rest steps of it could be phase two. Phase one is the preparation for the pre-process of system service after Ukey of consumers is inserted into the terminal device. And when Ukey disconnects the terminal, all the authentication and preparation information are invalid, and cryptography

service for the consumer is stopped. Phase two is the system management procedure when system service preparation is over, and according to the circumstances of cryptography service, VCM management scheduler adjust the status of cloud cipher machines through the way of migration with a regular time interval.

D. System Analysis

1) Availability analysis

Availability [13] of cloud computing system is usually considered from several kinds of service resources, namely, network resources, computing resources, storage resources, and so on. CC as a special case of cloud computing system, needs to consider the availability of cryptography resources in cloud environment additionally. CC virtualizes the underlying cryptography resource, network resource and computing resource into virtual resources that can be flexibly deployed. Owing to this, under the schedule of management platform, one cryptography component invalidated of CC will be replaced by another component rapidly, to ensure that quality of service provided by the upper application is not affected. CC adopts the pooling method upon cloud cipher machine cluster to convert cryptography resources and network resources into virtual resources that can be flexibly extended and configured [18], thereby improving the availability of cryptography cloud.

2) Security analysis

Security of CC need be considered from three layers, namely, infrastructure, platform and service. Infrastructure is a cluster of cloud cipher machines with hardware security module as trusted root to measure the credibility and integrity of system, thereby to ensure the trust and security of the upper system and protect the confidentiality and integrity of system data. Authentication module and certification authority module of CC provide a strategy of access control and a mechanism about key protection to maintain the stability of system and integrity of data from the perspective of malicious invasion. DEK is centralized by key escrow subsystem and encrypted by CMK that controlled by consumers, VCM would be allowed invoking the relevant keys after authenticated by system, to ensure system security standing on the platform management level. At the same time, a service-oriented security domain is set at network layer to implement logical isolation among consumers. Plaintext key only appears in HSM, and it is provided with hardware isolation and protection by root key to achieve confidentiality of keys. Relevant security technologies of CC need to be constantly perfected with the development of information technology, and it supports cryptography service in business cloud on the premise of ensuring itself security.

IV. Implementation and Experiment

A. Plan of Deployment

CC is based on OpenStack [14] that is a kind of cloud platform belong to open source. Which is similar to a cloud service infrastructure of Amazon, and there are correspondence and association between function modules of system and functional components of OpenStack. OpenStack includes four major functional components, who are Keystone that is authentication service, Glance that is image service, Neutron that is network management service, and Nova that is virtual machine management service. And OpenStack was developed secondly to become a management platform of CC [15]. Thereinto, Keystone corresponds with authentication module, Neutron corresponds with network manager, Glance and Nova was integrated into an organic whole that corresponds with monitor of cloud cipher machine and VCM management scheduler. KMC consists of several authentication servers with storage media to correspond with certification authority module and keys escrow module. CCC is composed of a cluster of cloud cipher machines and takes use of the redeveloped OpenStack to implement deployment of cryptography cloud.

B. Environment of System

Cloud cipher machine is composed by Inspur server and Intel accelerator. There are 4 sets of Inspur server, whose model number is NF5270M4, and the motherboard is Intel C610, there are six sets of PCI-E 3.0 expansion slot, a couple of 6-core processer, whose model number is Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz. Besides, there are memory that is a total of 128GB, a couple of Gigabit Ethernet, and tetrad SSD disks that is a total of 4TB. Per server is inserted with six accelerators, whose model number is Intel Corporation DH895XCC Series QAT. KMC is composed of a couple of authentication server, whose model number is Net Attest EPS ST 01.

Cloud cipher machine is deployed with Linux operating system, whose version is CentOS7-x86_64-1511, kernel version in which is Linux 3.10.0; OpenStack version is the most stable Newton. Authentication server supports trusted computing technology, with professional CA functions.

C. Implementation of VCM

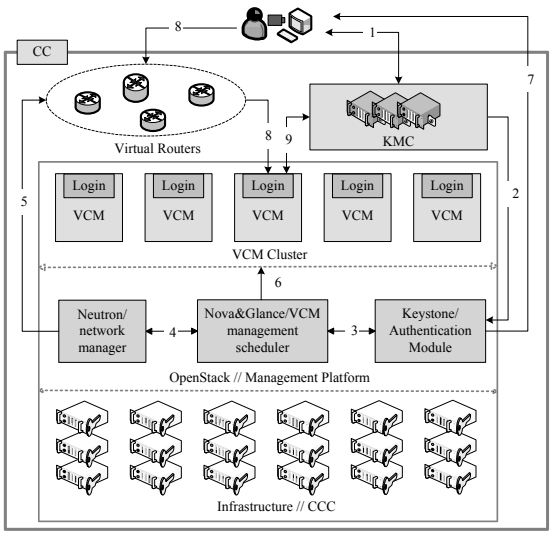

Figure 7. The management process of VCM

The core feature of the redeveloped OpenStack is infrastructure management of cryptography services, there are primarily creation, migration and deletion of VCM. Figure 7 is the management process of VCM. Thereinto, the migration of VCM has been described in section 2.3.3, not as the focus in the initial stage of research. the primary study is the implementation of basic functions of system, which is the creation and deletion of VCM.

The process of creating VCM by users is described as following pseudocode:

```
Process   Creation of VCM
INPUT   USER ID                    //*from USBkey*//
        build_vcm_request()   //*from business VM*//
Step one
    If USBkey TRUE
        ID→Terminal
    Then
        Terminal responding
        auth_identity_request()→KMC
    build_vcm_request()→KMC
        //*A→B is interpreted as that A is delivered into B*//
Step Two
    KMC responding
    If ID TURE
        user_vcm_token is generated
        user_vcm_token→Keystone
Step Three
    Keystone responding
    user_vcm_token is writed into Keystone_Database
    user_vcm_token→Nova
Step Four
    Nova responding
    user_vcm_ID is generated
    secure-region_deploy_request()→Neutron
    instance_build_order()→Glance
Step Five
    Neutron responding
    secure-region_info() defines vcm_virtual-net
Step Six
    Glance responding
    VCM-Image is generated
    return build_successful→Keystone
Step Seven
    Keystone responding
    login_permit() is generated
    login_permit()→Terminal
Step Eight
    Terminal responding
    Login()→VCM_instance
Step Nine
    VCM_instance responding
    Terminal responding
    KMC responding
CRYPTOGRAPHY SERVICE OF THE USER (ON)
```

The process of deleting VCM by users is described as following pseudocode:

```
Process   Deletion of VCM
INPUT   USER ID                    //*from USBkey*//
        deleted_vcm_request() //*from business VM*//
Step one
    If USBkey TRUE
        ID→Terminal
    Then
        Terminal responding
        auth_identity_request()→KMC
        delete_vcm_request()→KMC
          //*A→B is interpreted as that A is delivered into B*//
Step Two
    KMC responding
    If ID TURE
        user_vcm_token is deleted
        token_delete()→Keystone
Step Three
    Keystone responding
    user_vcm_token is deleted from Keystone_Database
    instance_delete()→Nova&&Glance
Step Four
    Nova responding
    secure-region_delete_request()→Neutron
    instance_delete_order()→Glance
    user_vcm_ID is deleted
Step Five
    Neutron responding
    Secure_delete_info is generated as Deletion Plan
    then
    vcm_virtual-net is deleted
Step Six
    Glance responding
    VCM-Image is deleted
    return delete_successful→Keystone
Step Seven
    Keystone responding
    delete_permit() is generated
    delete_permit()→Terminal
Step Eight
    Terminal responding
    PRINT "NO CRYPTO-SERVICE OFFER"
CRYPTOGRAPHY SERVICE OF THE USER (OFF)
```

D. Experiment of Performance

The main purpose of experiment is to evaluate VCM performance. Within the system, it creates 40 VCMs, and each VCM runs task queue that yield to Poisson Distributed in a loop. Object of encryption speed test are AES and SHA256, because the encryption and decryption speed of asymmetric algorithm is nearly one thousand times slower than that of symmetric algorithm, the test of asymmetric algorithm is of little significance. The result of experiment is shown in Figure 8.

Figure (a)-(c) of 8 show the encryption speed of AES, Hash and Null that tested in the VCM or Host with different modulus**.** From the figure (a), Null byte that with different modulus is encrypted by crypto card that in VCM or Host, the encryption speed is similar, even to be equal. So that, VCM does not has much loss on transfer mechanism, and can basically achieve the cryptography service which is close to quality of service that provided by Host. While if bytes are encrypted by AES, the encryption speed of VCM would be little slower than that of Host, but the quality of service can't be reduced. According to which, it can be concluded that symmetric algorithms that applied on the data encryption service can maintain the efficiency of cryptography service. However, if bytes are encrypted by Hash, the encryption speed of VCM would be reduced by more than twenty percent liken to that of Host, and even to fifty percent. But, the D-value could be the cost of transfer mechanism, because of the difference of dimensions of encryption speed in figure (a)-(c). It can be realized that CC has the characteristics of high-availability, and it can satisfy

cryptography service demand in the cloud environment. But in the aspect of virtual network transmission mechanism, there is still much issues to improve.

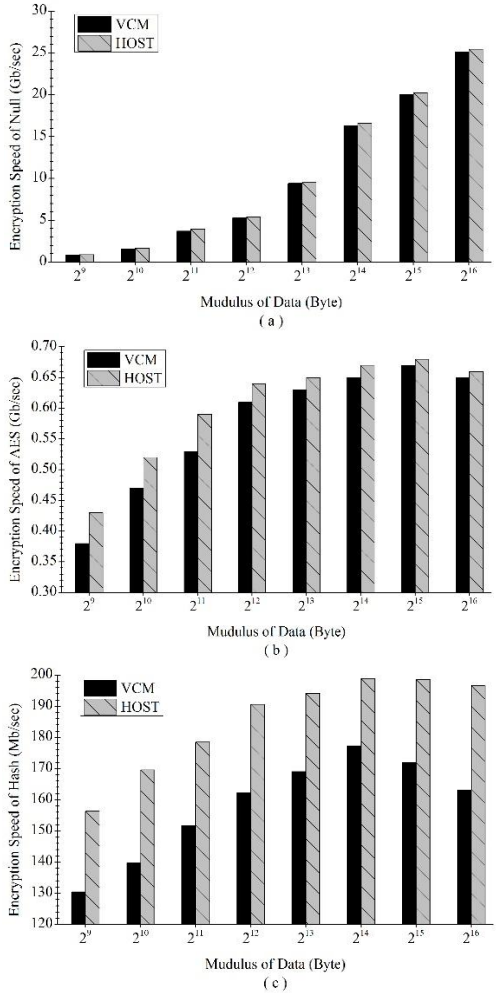

Figure 8. The result of encryption speed experiment

V. CONCLUSION

The continuous development of ciphergraph has come to the stage of cloud cryptography service. Cryptography service is moving in the direction of standardization, systematism and industrialization. The design scheme of CC framework is proposed in this paper, which provides the idea that offering cryptography service with cloud computing model to the consumers. It solves the problem of the incompatibility of traditional ciphergraph in the cloud environment and overcomes the limitations of carrier of traditional cryptography service system to expand and share cryptography resource. However, there are still many scientific problems need to be studied urgently, such as key transfer problem in the scheduling process of cryptography resources and key storage problem in the sharing process of cryptography resource, and so on.

ACKNOWLEDGMENT

This work was supported by National Key Research Program of China “Collaborative Precision Positioning Project”. (No. 2016YFB0501900).

REFERENCES

[1] ZHANG Y, CEN R, SHEN Y, et.al. *The Application of Cryptography Resource System in Cloud Computing* [J]. Journal of Information Security Research, 2016, 2(6):558-561.

[2] SUN L, DAI Z. *Research on Framework of Security Service Cloud Computing* [J]. Journal of Computer Applications, 2012, 32(1):13-15.

[3] Wang M, Liu L. *CRYPTO AS A SERVICE*[C]//THE 2th International Workshop on Cloud Computing and Information Security. Atlantis Press. shanghai: CCIS, 2013:152-155.

[4] National Institute of Standards and Technology. *The NIST definition of cloud computing. Technical Report*, No.800-145, 2011.http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[5] ZHANG Y, WANG X, LIU X, et.al. *Survey on Cloud Computing Security* [J]. Journal of Software, 2016, 27(6):1328-1348.

[6] AWS Support Center. *AWS CloudHSM User Guide* [EB/OL]. Seattle: Amazon Web Services, Inc. or its affiliates.2017[2017-12-02]. https://docs.aws.amazon.com/cloudhsm/latest/userguide/cloudhsm-user-guide.pdf

[7] QI K. *The first Cloud Data Encryption Service released by Alibaba Cloud and JN TASS* [J]. Information Security and Communications Privacy, 2016(1):87-87.

[8] KOU W, CHEN L. General *High-Performance Cryptographic Service System Model* [J]. MICROELECTRONICS & COMPUTER, 2016, 33(10):87-90.

[9] WANG Z, SUN L, GUO S. *Real-time Task Threshold Scheduling Method for Cryptography Cloud based on Rolling Optimization* [J]. Journal of Computer Applications, 2017, 37(10):2780-2786.

[10] LIU G, WU B, ZHANG Y. *Research on Key Techniques of Trusted Server Platform in Cloud Environment* [J]. Journal of Information Security Research, 2017, 3(4):323-331.

[11] Dong Y, Yang X, Li J, et al. *High-performance network virtualization with SR-IOV*[C]// IEEE, International Symposium on High PERFORMANCE Computer Architecture. IEEE, 2010:1471-1480.

[12] LIU W, QIU X, WANG X. *Software Defined Security -SDN/NFV Disclosure of New Network Security* [M]. Beijing: China Machine Press, 2017.

[13] LU W, CAI X, WANG H. *Discussion on Availability Analysis of Cloud Computing System* [J]. Information and Communication technologies, 2015(2):16-21.

[14] YI Y. OpenStack: Open Source Cloud[M]. Beijing: Tsinghua University press, 2014.

[15] YANG S G, ZHANG Y Y. A cloud computing resource pool system and its implementation: CN, CN103581324A[P]. 2014-02-12.

[16] FENG D G, ZHANG M, ZHANG Y, et al. Study on cloud computing security[J], Journal of Software, 2011, 22(1):71-83.

[17] ZHANG Y, QIN R W, SHEN Y C, et al. The application of cryptography resource system in cloud computing[J]. Journal of Information Security Research, 2016, 2(6): 558-561.

[18] WANG B F, SU J S, CHEN L. Review of the design of data center network for cloud computing[J]. Journal of Computer Research and Development, 2016, 53(9):2085-2106.

[19] https://help.aliyun.com/document_detail/28357.html?spm=5176.product28341.2.1.8LMnOC.