भारतीय सूचना प्रौद्योगिकी संस्थान धारवाड़

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY DHARWAD

A REPORT ON

Cloud Cryptography

By

Pankaj Kumar

17BCS036

Under Guidance of

Dr. Uma S.

1. Scope of the Topic

I. ABOUT THE TOPIC :

Cryptography is the protecting technique of data from the unauthorized party by converting into the non-readable form. The main purpose of cryptography is maintaining the security of the data from third party or Cyber-attacks. There are following two types of algorithms such as:

(i) Symmetric key based algorithm (conventional key algorithm).
(ii) Asymmetric key based algorithm (public-key algorithm).

In the cloud computing environment, security is deemed to be a crucial aspect due to the significance of information stored in the cloud. The data can be confidential and extremely sensitive. Hence, the data management should be completely reliable. It is necessary that the information in the cloud is protected from malicious attacks. Security brings in concerns for confidentiality, integrity and availability of data.

II. PROBLEM STATEMENT:

Customer's stores data at cloud service providers is vulnerable to various threats. In cloud computing, we consider four types of threat models:

a) **Availability**
b) **Integrity**
c) **Confidentiality**
d) **Reliability**

First is the single point of failure, which will affect the data availability that could occur if a server at the cloud service provider failed or crashed, which makes it harder for the customer to retrieve his stored data from the server. Availability of data is also an important issue which could be affected, if the cloud service provider (CSP) runs out of service.

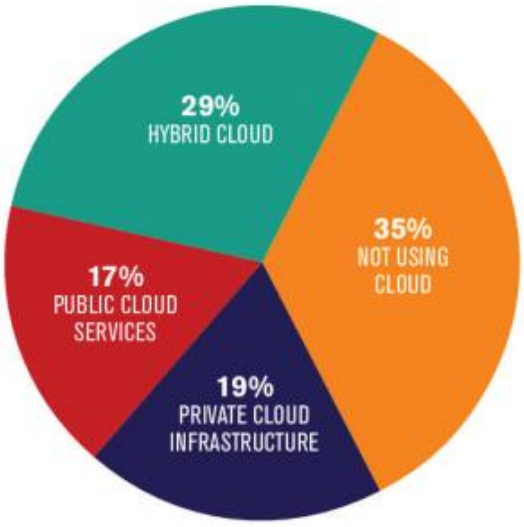
Our second threat is data integrity. Integrity is a degree confidence that the data in the cloud is what is supposed to be there, and is protected against accidental or intentional alteration without authorization. Such worries are no more beneficial issues; therefore,

a cloud service customer can not entirely rely upon a cloud service provider to ensure the storage of his vital data.

Most of the businesses that have held back from adopting the cloud have done so in the fear of having their data leaked. This feat stems from the fact that the cloud is a multi-user environment, wherein all the resources are shared. It is also a third-party service, which means that data is potentially at risk of being viewed or mishandled by the provider. It is only human nature to doubt the capabilities of a third-party, which seems like an even bigger risk when it comes to businesses and sensitive business data. There are also a number of external threats that can lead to data leakage, including malicious hacks of cloud providers or compromises of cloud user accounts. The best strategy is to depend on file encryption and stronger passwords, instead of the cloud service provider themselves.

III. Application to the real world

Cloud computing is a platform for expanding capabilities and developing potentialities dynamically without employing new infrastructure, personnel, or software systems. In Addition, cloud computing originated from a commercial enterprise concept, and developed into a flourishing IT invention. However, given that considerable information on individuals and companies are identified in the cloud, concerns have been raised regarding the safety of the cloud environment. Despite the hype surrounding cloud computing, customers remain reluctant to deploy their commercial enterprise into the cloud.



Some of the cloud Security services providers are.

2. Literature Study

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.

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.

3. New proposed Solutions - Research papers

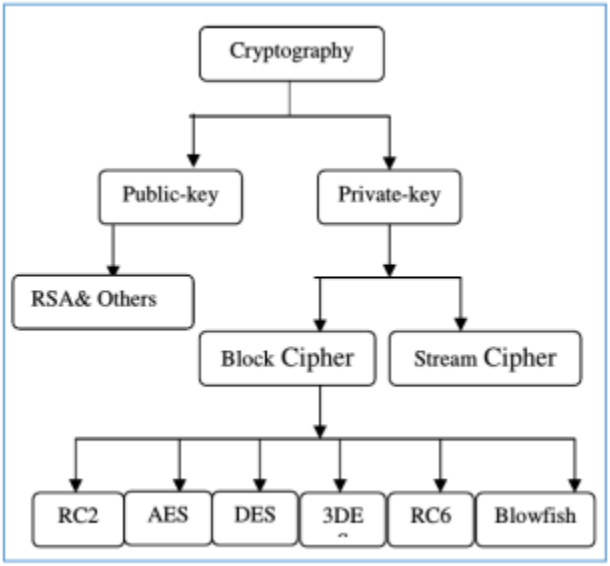
3.1 SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY, IRJET.

Mar-2018

- **Proposed Solution**

In this paper Author aim to securely store information into the cloud, by splitting data into several chunks and storing parts of it on cloud in a manner that preserves data confidentiality, integrity and ensures availability.

The Author's approach ensures the security and privacy of client sensitive information by storing data across single cloud, using AES, DES and RC2 algorithm.



- **FRAMEWORK**

  - **Data Encryption Standard:**

DES is the archetypal block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits.

In the **encryption** process, the data is first divided into 64-bit long blocks. Then, each block undergoes the following operations:

1. Initial permutation rearranges bits in a certain, predefined way. This step does not enhance the security of algorithm. It was introduced to make passing data into encryption machines easier, at the times when the cipher was invented.
2. The input data is divided into two 32-bit parts: the left one and the right one.
3. 56 bits are selected from the 64-bit key (Permutation PC-1). They are then divided into two 28-bit parts.
4. Sixteen rounds of the following operations (so called Feistel functions) are then performed:
    1. Both halves of key are rotated left by one or two bits (specified for each round). Then 48 subkey bits are selected by Permutation PC-2.
    2. The right half of data is expanded to 48 bits using the Expansion Permutation.
    3. The expanded half of data is combined using XOR operation with the 48-bit subkey chosen earlier.
    4. The combined data is divided into eight 6-bit pieces. Each part is then an input to one of the S-Boxes (the first 6-bit part is the input to the first S-Box, the second 6-bit part enters the second S-Box, and so on). The first and the last bits stand for the row, and the rest of bits define the column of an S-Box table. After determining the location in the table, the value is read and converted to binary format. The output from each S-Box is 4-bit long, so the output from all S-Boxes is 32-bit long. Each S-box has a different structure.
    5. The output bits from S-Boxes are combined, and they undergo P-Box Permutation.
    6. Then, the bits of the changed right side are added to the bits of the left side.
    7. The modified left half of data becomes a new right half, and the previous right half becomes a new left side.
5. After all sixteen rounds, the left and the right halves of data are combined using the XOR operation.
6. The Final Permutation is performed.

During **decryption**, the same set of operations is performed but in reverse order. The subkeys are also selected in reverse order (compared to encryption).

Weak keys in DES

A weak key in the DES cipher is a key which generates the same subkeys in all the successive rounds of encryption algorithm. There are four known weak keys in DES (expressed in hexadecimal):

- `0x00000000000000` (only zeros)
- `0xFFFFFFFFFFFFFF` (only ones)
- `0x0000000FFFFFFF` (only zeros and ones)
- `0xFFFFFFF0000000` (only ones and zeros)

Semiweak keys in DES

A semiweak key in the DES cipher is a key for which one can find another key that produces the same encrypted ciphertext from the same given plaintext. There are twelve known semiweak keys in DES (expressed in hexadecimal, along with parity bits):

- `0x01E001E001F101F1` and `0xE001E001F101F101`
- `0xFE01FE01FE01FE01` and `0x01FE01FE01FE01FE`
- `0x1FE01FE00EF10EF1` and `0xE01FE01FF10EF10E`
- `0xE0FEE0FEF1FEF1FE` and `0xFEE0FEE0FEF1FEF1`
- `0x1F011F010E010E01` and `0x011F011F010E010E`
- `0xFE1FFE1FFE0EFE0E` and `0x1FFE1FFE0EFE0EFE`

❖ **Advanced Encryption Standard**:

AES is a subset of the Rijndael cipher developed by Belgian cryptographers, VincentRijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes.For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

AES Encryption

During encryption, the input data (plaintext) is divided into 128-bit blocks. The blocks of data are presented as column-major matrices of size 4 bytes × 4 bytes, called states. The following operations are performed for all blocks:

1. Preparing Subkeys: one starting subkey is created first, and later one more subkey for every subsequent cycle of encryption (see below).
2. Initial Round: all bytes of data block are added to corresponding bytes of the starting subkey using XOR operation.
3. A number of encrypting cycles takes place. The number of repetition depends on the length of a secret key:
   - **9** cycles of repetition for a 128-bit key,
   - **11** cycles of repetition for a 192-bit key,
   - **13** cycles of repetition for a 256-bit key.

   The following operations are performed during each encryption round:
   1. Each byte of the state matrix is replaced with another byte, based on a lookup table, called Rijndael's S-Box. The operation is called the SB (Substitute Bytes) Operation. The construction of the lookup table guarantees that this substitution is non-linear.
   2. The bytes stored in the last three rows of the state matrix are shifted to the left. Note, that the bytes in the first row are not shifted at all. The bytes in the second row are shifted by one position, in the third row by two positions, and the bytes in the fourth row are shifted by three positions to the left. The leftmost

bytes in each row moves to the right side of the same row. This state is called SR (Shift Rows) Operation.

3. MC (Mix Columns) Operation (the multiplication of columns): all columns are multiplied with a constant matrix of size 4 bytes × 4 bytes.
4. AR (Add Round Key) Operation: adding XOR all state bytes to the subkey bytes. A new subkey is created for every encryption round. Subkeys, like states, are 16-byte long.

4. Final Round: the same operations are performed as in normal encryption rounds (described above), besides the multiplication of columns, which in the Final Round is omitted.

AES Decryption

During decryption, the encrypted text is used as input data to the algorithm. The corresponding, inverse operations should be performed, as during encryption:

1. Inverse bytes substitution (**ISB**).
2. Bytes shifting to the right (**ISR**).
3. Adding XOR to a subkey (**IAR**).
4. Inverse multiplication of columns (**IMC**).

Rivest Cipher 2 Algorithm (RC2):

In cryptography, RC2 (also known as ARC2) is a symmetrickey block cipher designed by Ron Rivest in 1987. "RC" stands for "Ron's Code" or "Rivest Cipher"; other ciphers designed by Rivest include RC4, RC5, and RC6.

The development of RC2 was sponsored by Lotus, who were seeking a custom cipher that, after evaluation by the NSA, could be exported as part of their Lotus Notes software. The NSA suggested a couple of changes, which Rivest incorporated. After further negotiations, the cipher was approved for export in 1989.

Keystream Initialisation

Initialisation a **T** table, used for generation of keystream bytes. **K** is the secret key, that is an array of length **k_len**.

```
for i from 0 to 255
    T[i] := i
endfor
x_temp := 0
for i from 0 to 255
    x_temp := (x_temp + T[i] + K[i mod k_len]) mod 256
```

```
        swap(T[i], T[x_temp])
    endfor
```

Keystream Generation

For keystream bytes generation, the loop below is executed as long as new bytes are needed.

```
p1 := 0
p2 := 0
while GeneratingOutput
    p1 := (p1 + 1) mod 256
    p2 := (p2 + T[p1]) mod 256
    swap(T[p1], T[p2])
    send(T[(T[p1] + T[p2]) mod 256])
endwhile
```

3.2 Research and Design of Cryptography Cloud Framework, IEEE. Aug – 2018

- **Proposed Solution**

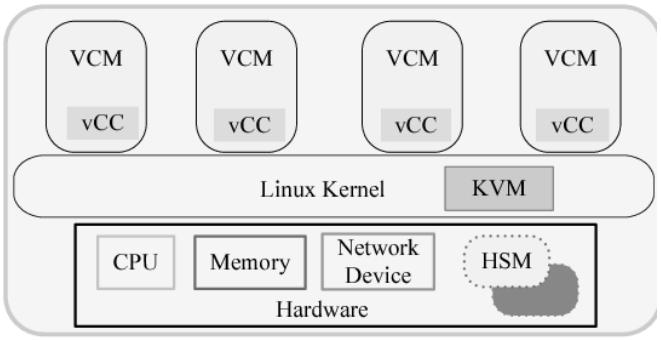
Since the application mode of cryptography technology currently has different types in the cloud environment, a novel cryptography cloud framework was proposed, due to the non-expandability of cryptography resources. Through researching on the application models of the current encryption technology, 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.

- **FRAMEWORK**

  - **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.



❖ Design of CC Framework

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. Given Figure 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. 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.

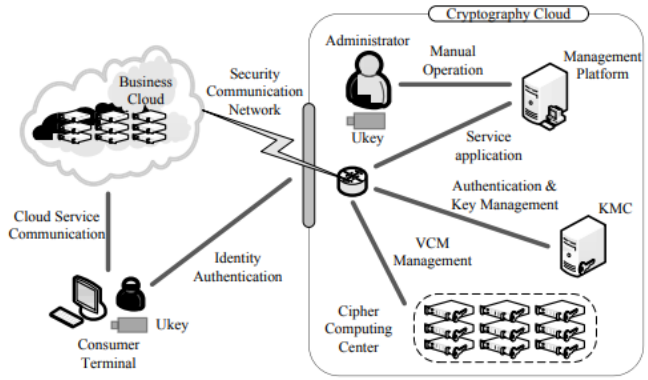


Figure 4. Service mode of Cryptography Cloud

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 to expand cryptography computing capabilities of CC.

Given Figure 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

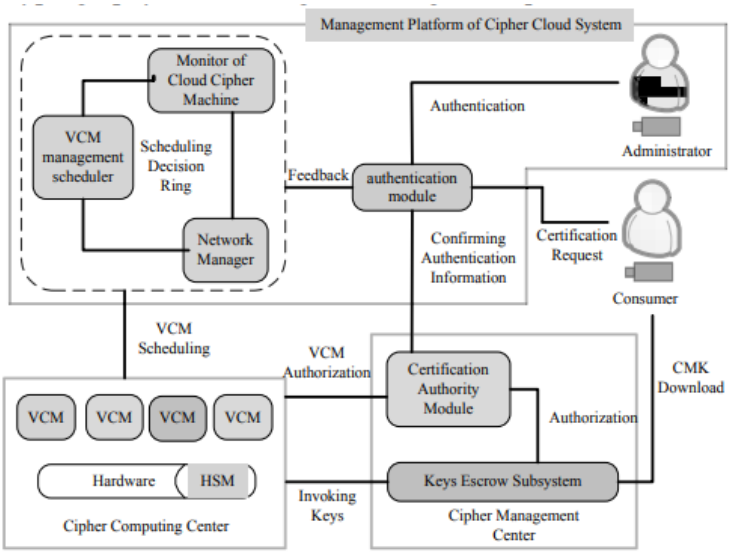


Figure 5. Functional modules of Cryptography Cloud

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.

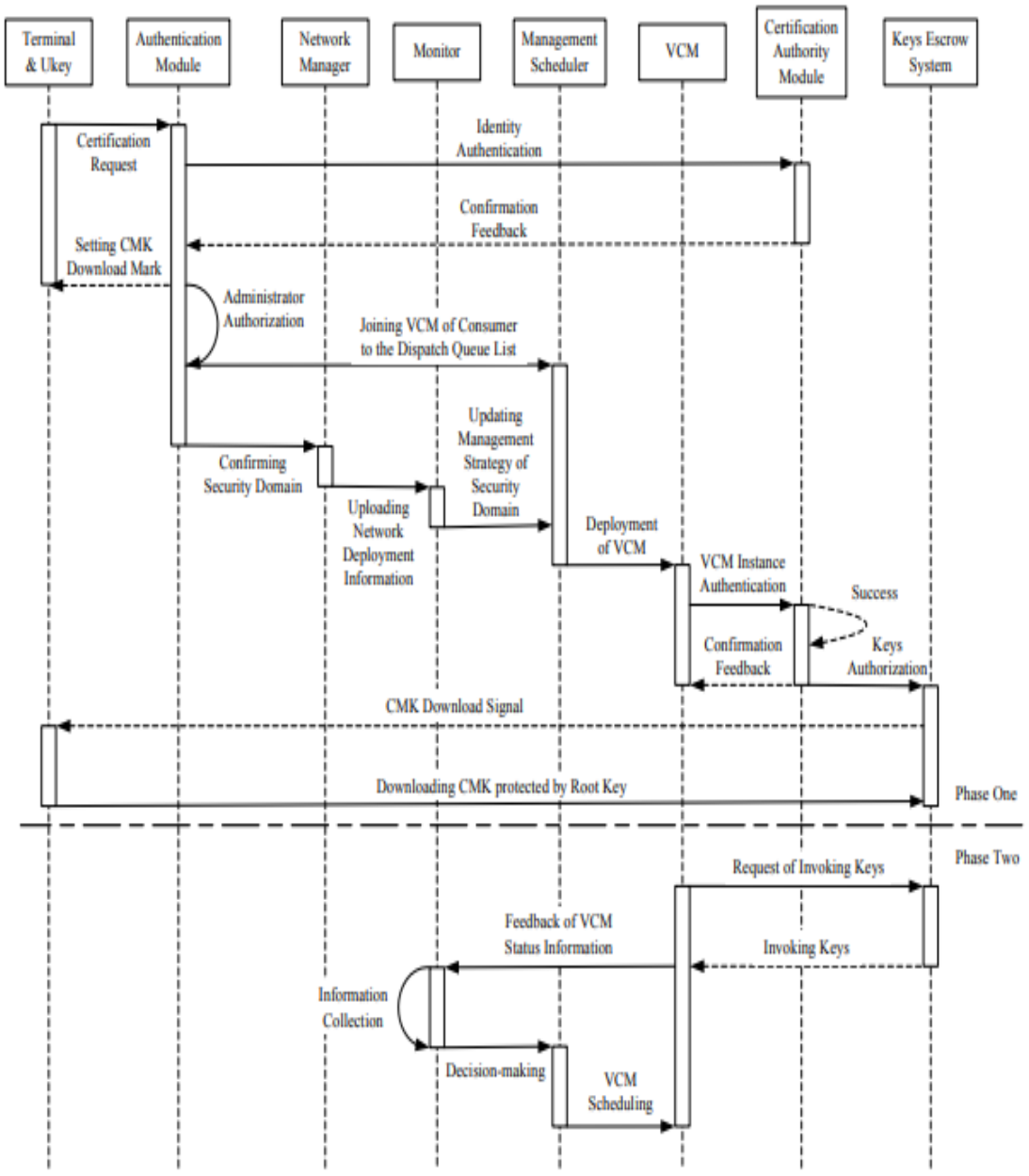


Figure 6. Cryptography service flow

Refreances

Paper 1

[1]VijayaPinjarkar, Neeraj Raja, KrunalJha,AnkeetDalvi, “Single Cloud Security Enhancement using key Sharing Algorithm, ”Recent and Innovation Trends in Computing and Communication, 2016.
[2] V. Vankireddy, N. Sudheer, R. Lakshmi Tulasi, “Enhancing Security and Privacy in Multi Cloud Computing Environment, ”International Journal of Computer Science and Information Technologies, 2015.
[3] Swapnila S Mirajkar, Santoshkumar Biradar, “Enhance Security in Cloud Computing, ”International Journal of Advanced Research in Computer Science and Software Engineering,2014.
[4] Ashalatha R, “A survey on security as a challenge in cloud computing,”International Journal of Advanced Technology & Engineering Research (IJATER) National Conference on Emerging Trends in Technology,2012.
[5]www.google.com
[6] G. L. Prakash, M. Prateek and I. Singh, ’Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System’, International Journal Of Engineering And Computer Science vol. 3, issue 4, pp. 5215- 5223, April 2014
[7] N. Saravanan, A. Mahendiran, N. V. Subramanian and N. Sairam, ’An Implementation of RSA Algorithm in Google Cloud using Cloud SQL’, Research Journal of Applied Sciences, Engineering and Technology, Oct. 1 2012

Paper 2

[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/cloudhsmuser-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.