Journal of Engineering Sciences

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

THE FUNCTION OF CRYPTOGRAPHY FRAMEWORK PLAN IN CLOUD COMPUTING

[1]Sameera Begum, [2]Dr. G. Kalaimani
[1]PG Scholar, MTech, Dept of CSE, Shadan Women's College of Engineering and Technology HYD, T.S.
fatimasameera60@gmail.com
[2]Professor, Dept of CSE, Shadan Women's College of Engineering and Technology HYD, T.S.

Abstract— Since the application method of cryptography innovation as of now has various sorts in the cloud condition, a novel cryptography cloud framework was proposed, due to the non-expandability of cryptography assets. Through researching on the application models of the flow encryption innovation, the cryptography service demand under the haze condition and the virtual structure of the cloud cryptography machine, this paper planned the framework of the cryptography cloud framework that gives cryptography services the cloud figuring mode. the structure idea of the framework is elucidated from two aspects incorporate the capacity of modules and service stream of cryptography cloud, which brought about the improvement of the adaptability of the application of cryptography innovation in the cloud condition. Through the analysis of framework capacity and management mode, it illustrated the availability and security of cryptography cloud framework. It was demonstrated that cryptography cloud has the characteristics of high-availability in the implementation and test, and it can satisfy cryptography service demand in the cloud condition.

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

I. INTRODUCTION

At present, information innovation with the rapid improvement advances the musicality and pace of society. With the assistance of characteristics of cloud registering that incorporate high scalability, high reliability and adaptability, increasingly more application frameworks migrate to the cloud to sent, for achieving the goal of centralized management of data and productive utilization of assets. Cloud registering innovation has been generally utilized in the information arrangement of industry, finance and government, which greatly facilitates the work and life of individuals; at the same time, organize information has turned into an important strategic asset, whose security can't be underestimated. To ensure security of information data in the system condition, cryptography application mode under the haze processing condition turns out to be particularly important. While the traditional cryptography innovation is restricted to fixed carrier and non-scalable cryptography registering asset, with the goal that it can't satisfy the encryption necessities of massive cloud data[1].

The origination of Crypto as a Service (CaaS)[2][3] built up the idea of cloud registering from the aspect of information security, it finds another way for the application of the cryptography innovation in the cloud condition, also innovates the new technique. According to the report of cloud registering standard[4] distributed by the NIST in 2011, the security of cloud processing can be partitioned 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 gear and system gear bolstered by confided in innovation, also on the reliability and security of re-appropriating calculations; the research on cloud data security incorporates confidentiality, uprightness, consistency and reliability of cloud storage data; the major research on the security of cloud hardware with the virtualization are vulnerabilities of hardware facilities regarding virtualization, security conventions and strategy of virtualized system and security innovation of cloud asset pool as well as the upper virtual machine[5]. Cloud cryptography service suppliers that incorporate Amazon Web Services (AWS), Alibaba Cloud, JN TASS and Sansec have advanced high-available security arrangements of the cloud, for example, AWS CloudHSM service that is the first to be achieved commercialization. In addition to that, CloudHSM service mainly gives key management capacities to the AWS cloud, and hardware security module (HSM) in which has the capacity of storage and management of clients' private key, and has the characteristics of fast calculation and abnormal state security necessities[6] . Alibaba Cloud launched cloud data encryption service[7] jointed JN TASS, which is to give sound data security answers for clients that based on hardware figure machine affirmed by State Cryptography Administration (SCA). Sansec set forward a progression of cloud security arrangements from the point of view of infrastructure security, application platform security and system transmission security, all of which have the duty of a guarantee to ensure security of keys and the validity of cloud cryptography service.

At the present stage, a large portion of cryptography applications have given insurance of business application information by the cloud figure machine and other hardware gadgets. So that,

research on cloud cryptography service that is based on facilities with virtualization work is winding up gradually mature, however despite everything it lacks the cryptography service framework with cloud processing model to give cryptography services. In this manner, to improve the adaptability of cryptography service in cloud condition. this paper considered and planned a cryptography cloud (CC) framework, and analyzed its usability and security.

II. RELATED APPLICATIONS

As of now, the realization of cloud cryptography service mainly relied upon the sending of cryptography gear in cloud condition, for example, the cloud server with HSM built-in that AWS and HUAWEI had launched, the confided in server that was the innovation of INSPUR and the cloud security arrangement based on crypto card that was created by Sansec. Concentrated on the security of cloud data focus, it is the main answer for "three-in-one" cloud security hierarchy include hardware security, framework safety and software security, and which is based on security and reliability of the underlying confided in hardware gear. What's more, using the key with confidentiality and controllability, it could reinforce security insurance of the framework to give high security-level hardware encryption service for application data.

Structure of cryptography service framework has loads of sorts, which is mainly based on the traditional figure machine, also it has been unable to meet the prerequisites of data security under the present cloud computing condition. KOU[8] displayed a superior cryptography service model, through the plan of a bound together service interface and the corresponding cryptography sources scheduling algorithm, aiming to achieve brought together management for cryptography service assets of various figure machines. Be that as it may, it is as yet insufficient in the aspects of security management of keys and performance of cryptography service, for example, key security issues and performance isolation issues. Aiming at the security of keys, WANG[9] displayed a cryptography service framework based on the outsider that key management focus. Keys are put away in the outsider that is creditable, and access control strategy and authentication innovation are utilized to keep confidential information of clients from malicious tampering or pilferage. The illegal client accesses their very own key information according to their necessities, however trust of the outsider can't be measured impartially, so there are as yet existing security dangers to a limited degree. The wave of confided in server of INSPUR launched a fundamental answer for the trust issue of key management focus. From the BIOS to the hardware arrangement of server, and then to the operating framework and applications of framework, believed measurement innovation makes the basic hardware facilities of key management focus trustworthy fundamentally. Be that as it may, despite everything it couldn't dispose of misappropriation of the internal manager, and to fathom which, it needs to reinforce the constraints and management from the angle of arrangements and regulations[10].

Ciphergraph in cloud condition is applied in the entire cloud service hierarchy that include three layers, IaaS, PaaS and SaaS individually. And which gives cryptography assets and services to safety efforts utilized in the service hierarchy, including all kinds of cryptography algorithms, cryptography application interfaces and cryptography service conventions. AWS CloudHSM services, encryption services of Alibaba Cloud and key management services of HUAWEI all upheld by HSM, also, which is utilized as a key store carrier sent in cloud computing condition. as appeared in Figure 1, cryptography service mode.

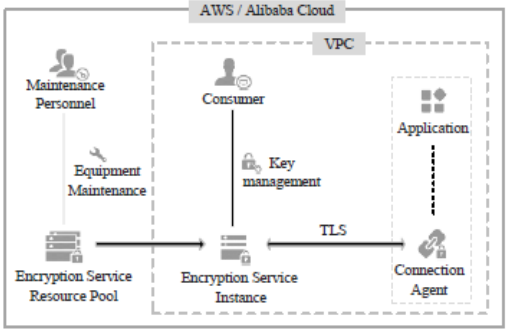


Figure 1. Cryptography service mode

Open cloud is made out of a plurality of virtual private cloud (VPC). The cloud encryption service asset pools are shaped by cloud figure machine bunch that bolstered virtualization capacities. And maintenance faculty are in charge of the maintenance of cloud figure machine and technical help. In addition, cloud encryption service asset pools interface with VPC through physical system, and furnish whom with cryptography service instances. Communications channel between business cloud and cryptography service instances are scrambled by security socket layer (SSL) convention to satisfy cryptography service need of business application. Key management service is the most important part in cloud condition, and to guarantee that the scrambled data of shopper is secure, it doesn't save encryption data key (DEK) that under the plaintext or ciphertext state which encoded by purchaser master key (CMK). CMK is constrained by customers to guarantee that cryptography service instances can

safely access DEK of clients. Figure 2 is the key management service architecture that is mainstream right now. Buyers can encode data by DEK that given by key management service (KMS) to guarantee that critical business data is secure. Therein to, business data is encoded by DEK, and DEK is scrambled by CMK that put away in key management focus (KMC), moreover, CMK is scrambled by root key based on HSM that as the base of trust to guarantee that root key can't be stolen from outside of the framework, in this manner, a total chain of trust can be organized. In addition, information channel is scrambled by transport layer security (TLS1.2) convention among HSM and KMS, and which among KMS and business to guarantee the reliability of the chain of trust.

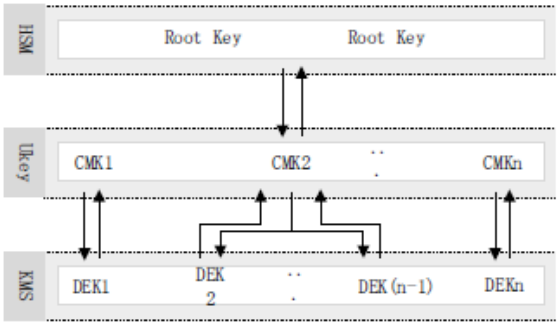


Figure 2. Key management service architecture

The advancement and application of cloud cryptography services rearranged the plan and implementation of cryptography service framework, with the goal that the utilization of ciphergraph in the cloud condition become normalized, and shoppers ordinarily need encryption and unscrambling operations to hold data. In addition, the management and dissemination of keys and credentials can exist as basic security services. Drawing on the characteristics of the present cloud cryptography services, and for that the cryptography service framework become progressively adapted to cloud computing condition, it is imperative to think about the cryptography service framework, which should be examined a further plan with key management work, adaptable expansion, easy to utilize, and meeting regulatory compliance prerequisites.

III. FRAMEWORK

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, The Proposed framework has following modules.

1. User Interface Design
2. User Authentication
3. Key Management Center
4. Encryption Process
5. Key Request

DESCRIPTION

1. User Interface Design

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

2. User Authentication

This is the first module of this project. In this module first user need to verify his Ukey which generated at the time of login. If the user enters valid Ukey user can go to home page. After that user send request to initialize VCM to store or retrieve the data. The KMC will provide VCM key. Then user needs to verify that key. If user enter right key the VCM is initialized at that particular instance. Every time user login user needs to initialize the VCM.

3. Key Management Center

This is the second module of this project. In this module all the keys will managed. Every time a Ukey will generate for every user. And VCM key will generate for every request of its initialization. And it will generate a root key in HSM, CMk key for user and DEK key when ever user wants to store the file in cloud. If any user wants to retrieve data from cloud user needs to request the final encrypted key.

4. Encryption Process

This is the third module of this project. In this module after user initialization of VCM then user stores the files. At the time of storing the file first root key will generated, then consumer master key will generated, the CMK key is encrypted with root key. Then encryption data key will generated, that DEK is encrypted with encrypted CMK. Then the file data is encrypted with the encrypted DEK. And it is stored in the database.

5. Key Request

This is the fourth module in this project. In this module after user initialization of VCM then user wants some file which is uploaded by other user. For that first user need to get the root key, DEK from the KMC for that user need to send the request to key management center. The KMC verify that whether the user accepted the request of user to download his file. If user accepted KMC provide the root key and DEK key to user to download the file.

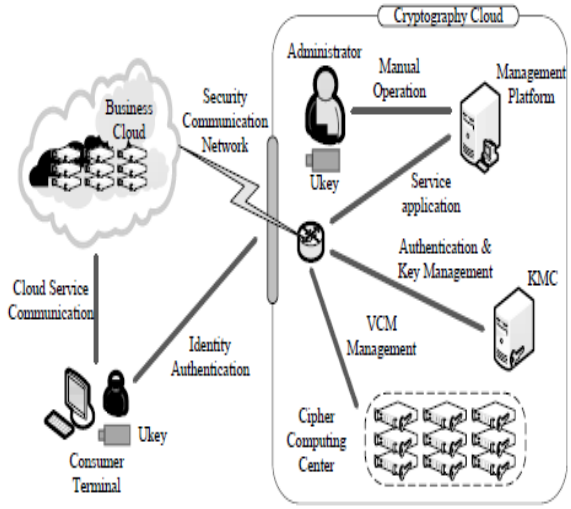


Fig. 3: Process of System

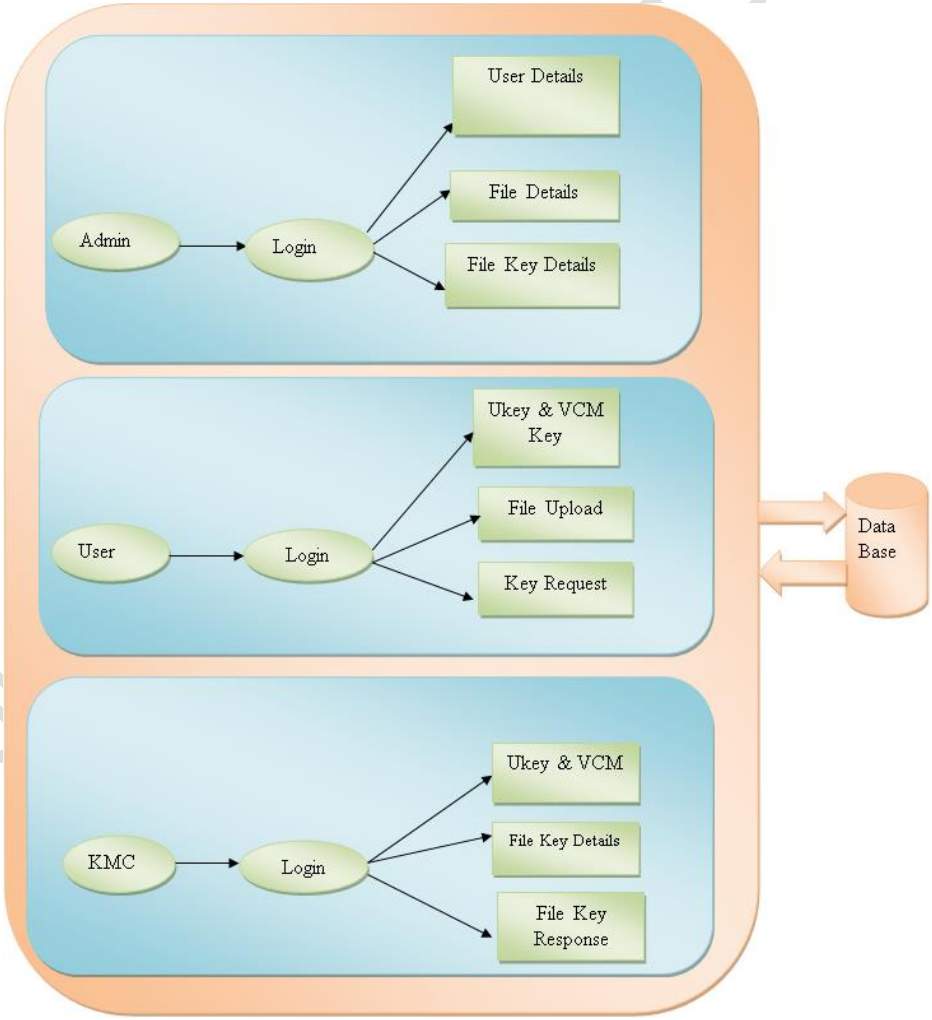
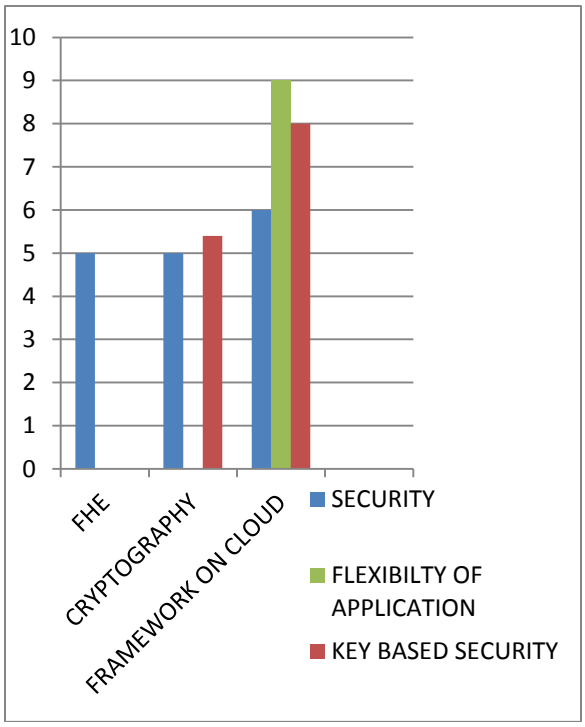


Fig. 5 System Architecture

IV. RESULTS:



V. CONCLUSION

The continuous improvement of ciphergraph has gone to the stage of cloud cryptography service. Cryptography service is moving toward standardization, systematism and industrialization. The structure plan of CC framework is proposed in this paper, which gives the idea that offering cryptography service with cloud computing model to the customers. It takes care of the issue of the incompatibility of traditional ciphergraph in the cloud condition and beats the limitations of carrier of traditional cryptography service framework to expand and share cryptography asset.

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.

AUTHOR'S PROFILE

Miss. SAMEERA BEGUM has completed her B.Tech from Green Fort engineering college, Bandlaguda, TS District, JNTU University Hyderabad. Presently, she is pursuing his Masters in Computer Science and Engineering from Shadan Women's college of Engineering and technology, Hyderabad, TS,India.

.

Guide Name:

Mrs. Dr. G. KALAIMANI has completed B.Tech (CSE) from Madras University, Tamil Nadu, M.Tech (CSE) from Mahendra engineering college, Anna University, Tamil Nadu , P.hd (CSE) from Mahendra engineering college, Anna University, Tamil Nadu Currently she is working as an Professor of CSE Department in Shadan Women's college of Engineering and technology, Hyderabad, TS. India