International Journal For Technological Research In Engineering
Volume 3, Issue 8, April-2016 *ISSN (Online): 2347 - 4718*

AN UPGRADATIONS OF HYBRID TECHNOLOGY FOR SECURING CLOUD DATA

Manish Mathur[1], Peeyush Mathur[2]
[1]PG Scholar, [2]Associate Professor, Sobhasaria Group of Institutions, Sikar

Abstract: In 2007, the concept of cloud computing, once made, it rapidly became a study in today's computer industry's hottest field and area to work. Its rapid popularization and sponsorship for the entire computer industry has brought a huge boost effect. But, we must clearly recognizing that the current cloud computing platform under development period, although a variety of cloud computing services platform has been recognized but are not grown-up sufficiently. Today, if we are think to establish the new IT industry. We require the lot of hardware device or software, and some other infrastructure for all kind of think; we need money to purchase the software license, different hardware device and also need dedicated staff members to maintain. Hence, there are not any such services, which provide the software desired to service users, but only user only require to use the software again when demand billing it. In this model of service, user only require paying an amount of rent to the service provider or supplier, you can get the proper services, based on the main concept, our main concept is the secure data (in database) on cloud platforms for that we use some encryption techniques to secure the data in database and we also use the hybrid techniques, load balancing techniques. Effective result can be seen in backend of application.

I. BACKGROUND

The first cloud computing project is launched the U.S. company Google, they launched a program called cloud computing. Google is also proposed basic theory and idea of the cloud computing [1].Many other corporations are introduced the own cloud computing plan for example yahoo, HP, or IBM and so on. They subsequently start on a new series of cloud including the concept of cloud security, cloud efficiency, private cloud or public cloud. Cloud cover from the bottom to the top level infrastructure at all level of the application layers, involving server, security or safety of data, networking, storage, and IT systems management. From the IT system analysis, cloud computing is totally different from the previous business model or commercial model, proposed & promotion of cloud computing will lead to a whole new industry of explosive growth. Finally, under this new business model will be able to make the user cloud computing, s/w application and data storage, management service as a regular service or facility, like modern peoples make use of the gas, water and electricity as usual [2]. Cloud express is one of the earliest technology companies to join the development and business application of cloud computing platform of the company. Cloud express platform used for business purposes, a development of cloud computing platform services. This platform is actually a solution for the improvement of the efficiency of data integration; operators can build their own data service center operation, through the center to integrate transportation camp data [3] [4].

The purpose of data transmission and storage can support a variety of different platforms and operating systems to run simultaneously exist, the current state more advanced cloud computing platform.

Challenges and issues for cloud computing

- Quality of service guarantees
- Dependence on secure hyper visors
- Attraction to hackers
- Safety of virtual OSs in the cloud
- Encryption require for cloud computing
- Encrypting access to the cloud source control interface
- Encrypting administrative access to operating system instances
- Encrypting access to application and Encrypting application data at rest
- Data ownership issues

II. LITERATURE SURVEY

In the 1990s, the emergence of the internet makes the world into a world of inter connectivity, so I began to concentrate on execution of cloud computing. Cloud computing [12] in the industry, there are various definitions of cloud computing. Cloud computing concept develops in continuous manner so that there are large explanation of the cloud computing come from differ background of researcher and Engineers. They all are from different background so that the definition of cloud computing are not the same, so the final classification also different.

2.1 Framework and services in the form of cloud computing

Cloud computing allows the users to calculate the service providers through a unified interface to cloud computing platform provides access to on demand storage power and a variety of application software services, resources on a cloud platform is dynamically handy and allocated, this form is available through the internet service to the majority of users & enterprises, and the user do not know the overall structure and composition of the cloud [5]. Simple framework of cloud computing services is shown in figure 1.

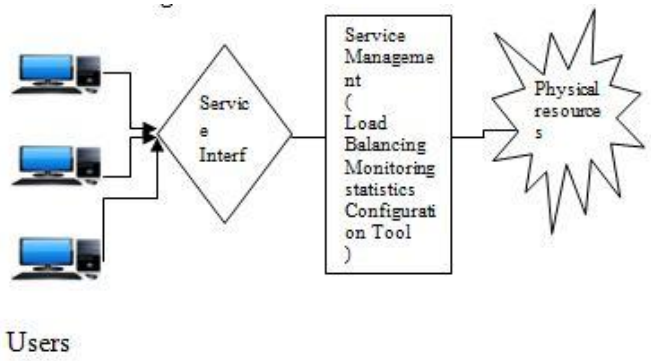

Fig. 1 The basic framework for cloud computing services.

As can be seen from figure 1, the basic architecture of cloud computing services, and cloud servers numerous huge. Additionally, cloud computing services can also take benefit of virtualization technologies, any device capable of getting right of entry from anywhere, as long as these devices must have internet connection, and also given that customized services for users. Cloud computing services overall architecture consists of users, service interfaces, service management, resources and physical resource. Users submit requests service; provides users with service interface of a cloud interface between; service management provides load balancing, monitoring, statistics and resource allocation and other services; physical resources is composed of several servers and hardware stores, and they need to connect the router configuration[6].

Cloud computing architecture includes two aspects: one is the infrastructure, which is at the bottom level to build a cloud computing, it is a foundation, is mainly used to build the upper application; hand is the application service programs, these programs sequence is used as the basis of the designed.Summed up under domestic and international published literature and current cloud computing research institute several types of services, cloud computing can be divided into the following four levels: the application layer, the platform layer, infrastructure layer and virtualization layers. Four service levels and each level correspond to cloud computing Services to be shown in Figure 2.

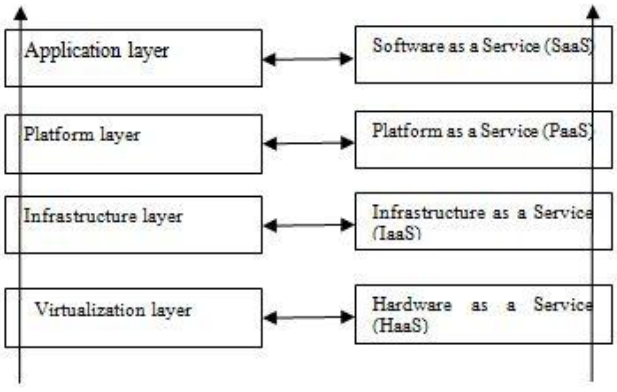

Fig.2 Cloud computing service levels and corresponding service.

2.2 The Core technology of cloud computing

Cloud computing is a new method of calculation, calculation is based on data-centric, the literature also points analysis of the differences between cloud computing and traditional way of supercomputing approach and summarizes results of three key cloud computing technology, That data storage and management technology, programming and technology virtualization[3] [7].

(1) Data storage or management technology

Most current storage technology platform uses a distributed cloud storage technology. High reliability of the data is generally storage through the use of backup methods to ensure that a copy of the data will also keep a copy in the cloud platform, multiple nodes.

(2) Programming Techniques

The main purpose of programming is to enable user to use cloud computing services platform for develop their own applications, so the cloud programming technology to users in the programming staff is crucial want by programming technology enables users to more easily programmed using cloud resources, allowing users to use the most convenient, belonging to the user's the easiest way to own program can be executed develop concurrently [8].

(3) Visualization Technology

Virtualization is a cloud computing resource management and scheduling reasonable technical basis of this technique is a virtual operating machine. A virtual machine is a way to simulate the operation of the hardware, but also the hardware to operate alternative software, so users can enough to run a choice of operating systems in virtual machines above, thereby obtaining and maintaining a class execution environment [9].

III. PROPOSE MODEL

Here we introduce our propose method techniques, which is work with the Hybrid Cloud concept. We use hybrid encryption techniques. Hybrid encryption is a mode of encryption that merges more than one encryption systems. It incorporates a combination of the symmetric & asymmetric encryption to benefit from the strengths of each form of encryption. These advantage or strengths are respectively defined as speed and security. Hybrid encryption is considered a highly secure and safe type of encryption as long as the private and public keys are fully secure.Hybrid encryption system is the simple communication model, as shown in Figure 3.

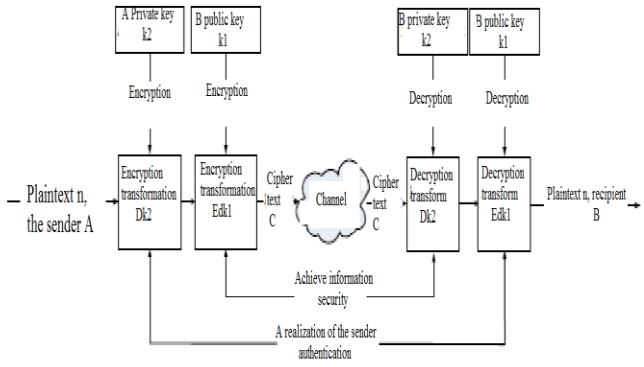

Fig 3: Hybrid encryption system for simple Communications Model

Symmetric and asymmetric key password systems have their own advantages and disadvantages. Symmetric key systems are significantly faster than asymmetric key password system, but require all parties to somehow share a secret key. The asymmetric algorithms allow key exchange systems / key-sharing system and public key infrastructures, but at the cost of speed.

A hybrid encryption system is a protocol jointly using multiple ciphers of different types, each to its best benefit and advantage. One common approach is to generate a random secret key for a symmetric and then encrypt this key via an asymmetric using the recipient's public key. The message itself is then encrypted via the symmetric and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient [10].

Hybrid encryption system is in order to better protected storage and data in transit, and it's biggest advantage is that security of higher than the above two institutional security is high. However, it also has some inevitable shortcomings, such as the following: Calculate the quantity is Large, slower processing speed, storage space is large, bandwidth requirements of higher. However, because of its high level of security feature, and the practical application the use of hybrid encryption systems often have more of a cryptographic system.

3.1 Improvement of hybrid-encryption-algorithm

The discussions of DES-algorithm, RSA-algorithms and ECC-algorithm explain that any of the algorithms for individual use are often not able to fully meet cloud computing requirements of security and efficiency. This thesis is the first three algorithm's advantages and disadvantages, and a based on DES algorithms and RSA, ECC algorithm to mix of encryption algorithm, which is symmetric-encryption algorithm and non-symmetric-encryption algorithm. The improvements of the algorithms are characterized by confidentiality, safely, encryption is fast, and is not vulnerable to the attack, and so on; you can guarantee the security of as much as possible to maximize efficiency. Improvements process of the hybrid encryption algorithm shown in Figure 4.

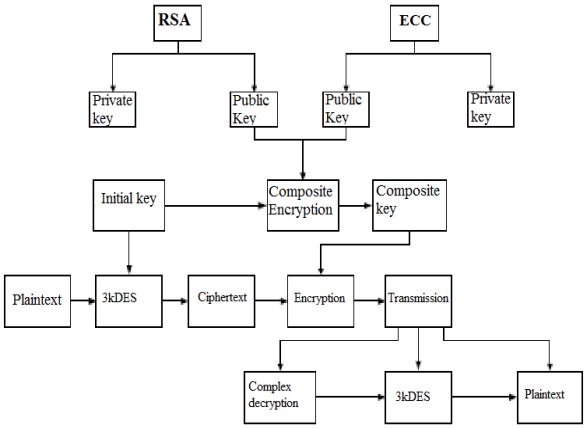

Fig4 Improvement of the hybrid Encryption Algorithm Processes

Due to DES encryption-algorithm has the benefits of fast speed and overcome the disadvantages of short key length, this thesis based on the DES-algorithm, designs a kind of improved hybrid encryption algorithm 3kDES [11].3kDES algorithm is, for the data packet or message three times DES encryption, this can increase key's length. Because the length of key is too small to avoid the attack caused by, while it remain the same benefit and DES encryption algorithm faster maintained. In multiple DES encryption key-pair while improved, Because DES during shift change even after 16 product transformation, each have a round with the same product transformation, each will use the same 48,Then after each round of the product at the time of conversion may have joined the 48 keys, this bit key, this key will be generated by the DES algorithm is 768, the total length after three DES keys will reach close the total length of the key will reach 2,304.This method can greatly increase difficulty of cracking, but also increases the security.

IV. IMPLEMENTATION OF THE HYBRID ENCRYPTION ALGORITHM

Improvement method of 3kDES hybrid encryption algorithm described below:

(1) The encryption process

First, assume the plaintext space A, A's size according to each group 64, 64 is not the complement of the random 64, after the packet plaintext space as: A_1 A_2 A... A_i. Next, for all packet encrypted according to 3kDES-algorithm, the cipher text set to B, the encryption process is:

$Bi= kDESx_3(kDESx_2^{-1}(kDESx_1(Ai)))$

After we get the whole space-A plaintext encrypted as B_1 B_2 B_3... B_i. An entire plaintext uses the 3DES, a process for the encryption algorithm:

$B=kDESx_3(kDESx_2^{-1}(kDESx_1(A)))$

The next set of keys were used in the first step in encrypted X_1, X_2, X_3 is encrypted using the RSA algorithm and the ECC combined. First, the X_1, X2, X3into $X_r$and X_s. Two parts, namely the use of ECC and RSA algorithms for the two parts of key groups encrypt:

(A) Encryption using the RSA algorithm for X_r and generating cipher text C_r

First set the RSA algorithm using large prime numbers has multiplied to n, the public key is set to m, the RSA for X_r

Encryption process is:

$C_r=X_r^m \bmod n$

(B) Encryption using the ECC algorithm for $X_s$and generating cipher text C_s

First set of elliptic curve Ep (a, b), select a basis point on the curve G finite fields, supposing ECC algorithm is key for k, choose a random number x, then the ECC for X_s

Encryption process is:$C_s=X_s+X_{kG}$

Where: kG public key algorithm for the ECC.

As a result the encryption process is complete, we can send an cipher text using 3kDES algorithm result as B, RSA encryption algorithm cipher text C_r and ECC algorithm encrypted cipher text C_s,

The final form of the cipher text is $B + C_r + C_s$.

(2) Decryption process

When recipient receive the cipher text B + C_r+ C_s, we start the decryption process. Firstly, we set the RSA algorithm uses a large prime number multiplied n and private key is d, the decryption process is

$X_r=(C_r)^d \bmod n$

We get X_r with the help of RSA algorithm. Secondly, we set the ECC algorithm C_s decrypt get X_s. it's the reverse process of ECC encrypted algorithm; the formula can be expressed as:

$X_s= C_s-X_{kG}$

Then we decrypt the cipher text B, in fact, the reverse process of the encryption, is calculated as:

$A = kDESx_1^{-1}(kDESx_2(kDESx_3^{-1}(B)))$

Thus the decryption process is completed, the finally obtained plaintext A.

4.1 The design of the node and load balancing

The core purpose is to service into traditional software online software services, which is one premise of protecting cloud computing gained popularity and promotion. This paper is designed for the node itself using the cache strategy. Cloud data is stored in the node itself, but because the overall number of nodes and the node's own resources are limited, and Cache design principles nodes is all the nodes in the storage can be seen as a cloud. Random walk algorithm, typical is a distributed load balancing algorithm. According to the algorithm devised between clouds node is equal relationship, no central node and the slave node difference design philosophy. The algorithm is that cloud server node.

V. PERFORMANCE ANALYSIS OF CLOUD COMPUTING SERVICE MODEL

Encryption algorithm to encrypt and decrypt, but at the same time will also consume some time encryption and decryption, also will consume part of the resources, the 3kDES algorithm and RSA, ECC algorithm to make a comparison and analysis of the performance, from and evaluate, the improved performance of this hybrid encryption algorithm.

Table 1 shows the three encryption algorithms are time-consuming for a small amount of data to compare data.

Computation time	3kDES	RSA	ECC
1st test	43ms	456ms	421ms
2nd test	44ms	432ms	452ms
3rd test	46ms	467ms	483ms
4th test	47ms	487ms	473ms
5th test	49ms	492ms	437ms
Average time	45.8ms	466.8 ms	453.2ms

Next is the large amount of data obtained in the test case, Table 2 shows the three encryption algorithms to encrypt the time spent large amounts of data comparison data.

Table 2 Three encryption algorithms to encrypt a large amount of data the time spent

Computing time	3kDES	RSA	ECC
1st test	9.587s	198.322s	156.422s
2nd test	10.132s	178.457s	168.569s
3rd Test	9.876s	187.684s	178.436s
4th test	10.324s	197.486s	163.924s
5th test	10.432s	189.798s	154.639s
Average time	10.070s	190.349s	164.398s

Through the analysis of test results shows that, 3kDES algorithm is a symmetric encryption algorithm is a symmetric cipher mechanism areas, it speed on the encryption is an obvious advantage. The test results in Table 1 and Table 2 conclusion can also verify this. So3kDES algorithm is suitable for large amounts of data to be encrypted. The RSA and ECC algorithm in the processing of information due to its inherent operational mode leads to a lot of time consuming, is not conducive to the large amount of data to encrypt data processing. Finally, it can be concluded: improved 3kDES and RSA, ECC algorithm hybrid encryption algorithm in terms of efficiency and performance symmetric encryption algorithm is basically the same, but in terms of security and public key encryption algorithm and fairly, this paper presents the change into the hybrid encryption algorithm to ensure higher security while improving the efficiency of encryption and decryption, can well assure cloud operator safety features of the service.

VI. CONCLUSION

Research work is summarized as follows:

(1) This paper discusses the current cloud computing security problems and pitfalls faced in terms of efficiency, pointed out the cloud safety and efficiency aspects of the issue is an important reason to get the current constraints of cloud computing to promote and popularize the. For two heavy these issue, this paperproposes a service model based on cloud computing platform, designed to improve the safety and efficiency of cloud computing platform.

(2) For the security issues of cloud computing, the paper secures transmission of data storage and data security for both aspects into line research. Cloud data security design into mass storage data storage and backup design methods and mechanisms designed to isolation.

REFERENCES

[1] Grover, J.; Shikha; Sharma, M. "Cloud computing and its security issues — A review", Computing,COMMUNICATION and Networking Technologies (ICCCNT), 2014 International Conference on, On page(s): 1 – 5

[2] Huang Jing; Li Renfa; Tang Zhuo "The research of the data security for cloud disk based on the Hadoop framework", Intelligent Control and Information Processing (ICICIP), 2013 Fourth

International Conference on, On page(s): 293 – 298
[3] Zeng Zeng; Veeravalli, B. "Do More Replicas of Object Data Improve the Performance of Cloud Data Centers?", Utility and Cloud Computing (UCC), 2012 IEEE Fifth International Conference on,On page(s): 39 – 46
[4] Srivastav S., Ram Kr. "Indirect method to measure software quality using CK-OO suites", IEEE-ISSP2013, 2-3 march 2013,ISBN:978-81-909376-6-5.
[5] W. Itani, A. Kayssi, A. Chehab "Privacy as a Service: Privacy-Aware Data Storage andProcessing in Cloud Computing Architectures"IEEE International Conference on Dependable,Autonomic and Secure Computing 2009 pp 711-716.
[6] Sanjay Ghemawat, Howard Gobioff, Shun-Tak Leung "The Google File System" Proceedings of the 19th ACM Symposium on Operating Systems Principles 2003 pp20-43.
[7] Fei Hu, MeikangQiu, Jiayin Li, etal "Review on cloud computing: Design challenges inarchitecture and security" Journal of Computing and Information Technology 2011, pp25-55.
[8] Chen Kang, Zheng Weimin "Cloud Computing: Examples and Research Status System" Journal of Software 2009, pp 1337-1348.
[9] Kaufman, "LM Data Security in the World of cloud computing" Security & Privacy, IEEE,2009, pp: 61-64.
[10] Foster I, Zhao Y, Raicu I, et al. "Cloud Computing and Grid Computing 360-Degree Compared" IEEE Grid Computing Environments Workshop. NJ USA, IEEE Computer Society,2008: 1-10.
[11] L Wang, J Tao, M Kunze "Scientific Cloud Computing: Early Definition and Experience", Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, Dalian, China, 2008, PP:825-830.
[12] Y. Murata, T. Inaba, H. Takizawa, H. Kobayashi, "A distributed and cooperative load balancing mechanism for large-scale p2p systems". SAINT Workshops, International Symposium on Applications and the Internet Workshops 2006.

