IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Dynamic Migration of Content Distribution Services for Minimum Cost using AES

Prof. Hema Kumbhar[1], Nishigandha Rajhans [1], Lalita Sonawane[1], Vedika Dhage[1], Nitesh Vanarase[1]

Department of Computer Science, Savitribai Phule Pune University[1]

Abstract: Now a days, cloud computing is most popular network in world. Cloud computing provides resource sharing and online data storage for the end users. The main issue is to best utilize the cloud as well as the application provider's existing private cloud, to serve volatile requests with service response time guarantee at all times, while incurring the minimum operational cost. Employing Lyapunov optimization techniques, we design a dynamic control algorithm to optimally place contents and dispatch requests in a hybrid cloud infrastructure spanning geo-distributed data centers, which minimizes overall operational cost over time, subject to service response time constraints. Also there are many security issues while migrating the data within the clouds. So, security becomes essential part for the data which is stored on cloud. To solve this issues, the paper presents AES encryption and decryption technique. AES is high secured and fastest technique. This infrastructure guaranteed to secure the information and minimizes the operational cost in cloud server.

Index Terms: Cloud computing, Content Distribution, Lyapunov Optimization, Dynamic Migration, AES Algorithm.

1. INTRODUCTION

Cloud computing technologies have enabled rapid provisioning and release of server utilities (CPU, storage, bandwidth) to users anywhere, anytime .To exploit the diversity of electricity costs and to provide service proximity to users in different geographic regions, a cloud service often spans multiple data centers over the globe, e.g., Amazon Cloud Front [1], Microsoft Azure [2], Google App Engine [3].

1.1 Cloud computing

Cloud Computing means Storing and accessing data and programs over the internet instead of computers harddrive. Cloud computing system is divided into 2 sections: The first section is known as front-end and another section is the back-end. They are connected to each other by using network which is called as the Internet. The front-end contains the computer of client (or computer network) and the system application is required to retrieve the cloud computing data. At the back-end of the system there are the several computer systems, several server nodes and data storage systems that developed the cloud of the computing service. The central server's task is to administrating the system, monitoring trace and client demands ensure that everything runs very correctly or not.

1.1.1 Cloud deployment models

- **Public Cloud**: A cloud in which a service provider makes resources (applications and storage) available to general public over the internet.
- **Private Cloud**: A cloud is a particular model that involves a distinct and secure cloud based environment in which only the specified client can operate.
- **Hybrid Cloud**: It is an integrated cloud service utilizing both private and public clouds to perform distinct functions within the same organization.

1.1.2 Cloud service models

- **Software as a Service**: (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network.
- **Platform as a Service: (**PaaS**)** is a model for delivering operating systems and associated services over the Internet without downloads or installation.
- **Infrastructure as a Service:** (IaaS**)** involves outsourcing the equipment used to support operations, including storage, hardware, servers and networking components.

1.2 Content distribution

A content delivery network or content distribution network (CDN) is a large distributed system of proxy servers deployed in multiple data centers via the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.

1.3 Lyapunov optimization

Lyapunov optimization is a powerful technique for optimizing time averages in stochastic queueing networks. Work in presents a drift-plus-penalty theorem that provides a methodology for designing control algorithms to maximize time average network utility subject to queue stability.

1.4Dynamic migration

Content Migration is the process of moving information stored on a Web content management system (CMS) within hybrid cloud.

1.5AES algorithm

It is a web tool to encrypt and decrypt text using AES encryption algorithm. You can chose 128, 192 or 256-bit

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

long key size for encryption and decryption. The result of the process is downloadable in a text file.

2. RELATED WORK

Migration of applications into clouds: A number of research projects have emerged in recent years that explore the migration of services into a cloud platform. Hajjat et al. [] develop an optimization model for migrating enterprise IT applications onto a hybrid cloud. In this paper, onetime optimal service deployment is considered, while our work investigates optimal dynamic migration over time, to achieve the long-term optimality.

Lyapunov optimization theory: Lyapunov optimization was developed from the stochastic network optimization theory and has been applied in routing and channel allocation in wireless networks, in a few other types of networks including peer-to-peer networks []. Maguluri et al. [] propose various VM configuration scheduling algorithms for cloud computing platforms that achieve arbitrary fraction of the capacity region of the cloud. But their model does not take into consideration delay guarantee, which is an important component in our optimization framework.

Chuan Wu.[] develop an optimal migration of content distribution services onto a hybrid cloud, such that the operational cost is minimized while service delay bound is guaranteed. While migrating the content, security is maintained using AES algorithm in this paper. Mr. Rahul Kamble [] propose Advanced Encryption Standard is the new best encryption algorithm by NIST to replace DES The size of key is unlimited, where the block size is maximum 256 bits. AES encryption technique is fastest, flexible and secured. It can be supported on various platforms.

3. SYSTEM MODEL

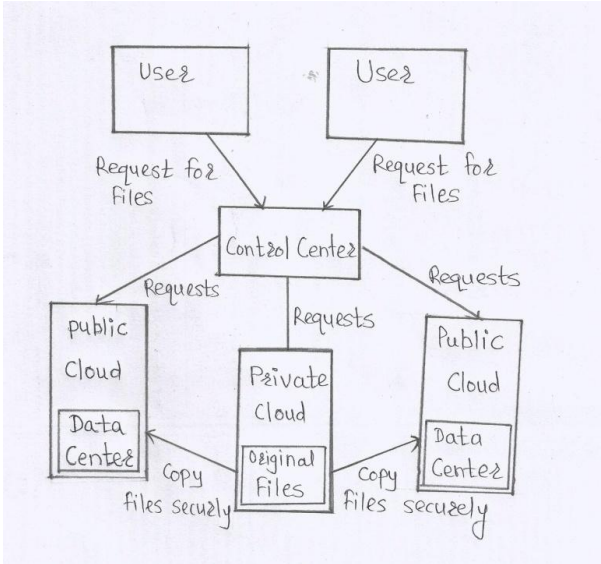

Fig1: System architecture

We consider a typical content distribution application, which provides a collection of contents (files), denoted as set M, to users spreading over multiple geographical regions. There is a private cloud owned by the provider of the content distribution application, which stores the original copies of all the contents. The private cloud has an overall upload bandwidth of b units for serving contents to users.

There is a public cloud consisting of data centers located in multiple geographical regions, denoted as set N. One data center resides in each region. There are two types of inter-connected servers in each data center: storage servers for data storage, and computing servers that support the running and provisioning of virtual machines (VMs). Servers inside the same data center can access each other via a certain DCN (Data Center Network).

The major components of the content distribution application include: (i) back-end storage of the contents and (ii) front-end web service that serves users' requests for contents. The application provider may migrate both service components into the public cloud: contents can be replicated in storage servers in the cloud, while requests can be dispatched to web services installed on VMs on the computing servers. An illustration of the system architecture is given in Fig. 1.

In existed system there are many security issues and security problems for data which is transmitted and stored on cloud. To solve this, we have used AES encryption and decryption techniques with single secret key.

In this system, if user use secret key for encryption then user should have use same secret key for decryption. This encryption and decryption will do within hybrid cloud. While decrypting data it access file from one cloud securely and decrypt at another cloud with single secret key which is used at encryption time.

Our objective in this paper is: (i) content replication: which content should be replicated in which data center at each time? (ii) Request distribution: How many requests for content should be directed to the private cloud and to each of the data centers that store this content at the time? (iii) Security while migrating the data: make sure while migrating the data is secured or not?

4. QUEUEING MODEL

We suppose that the system runs in a time-slotted fashion. Each time slot is a unit time which is enough for uploading any file $m \in M$ with size $v^{(m)}$ (bytes) at the unit bandwidth. In time slot t, $a^{(m)}$ j (t) requests are generated for downloading file $m \in M$, from users in region j. We assume that the request arrival is an arbitrary process over time, and the number of requests arising from one region for a file in each time slot is upper-bounded by Amax

The cost of uploading a byte from the private cloud is h. The charge for storage at data center i is pi per byte per unit time. gi and oi per byte are charged for uploading from and downloading into data center i, respectively. The cost for renting a VM instance in data center i is fi per unit time. .We also assumes that each request is served at one unit bandwidth, and the number of requests that a VM in data center i can serve per unit time is ri.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Decision variables. The decision variables in our optimization framework are formulated as follows: (1) For content replication, binary variable $y_i^{(m)}(t)$ indicates whether file m is stored in data center i in time slot t or not. If $y_i^{(m)}(t-1) = 0$ and $y_i^{(m)}(t) = 1$, file m is copied from the private cloud to the data center i at t; if $y_i^{(m)}(t-1) = 1$ and $y_i^{(m)}(t) = 0$, file m is removed from data center i. In other cases, the storage status remain the same. In case of migration.

M	File set
$a^{(m)}{}_j(t)$	No. of requests for file m from region j
$Q_j^{(m)}(t)$	Size of requests queue for file m in region j at t
$c_{ji}^{(m)}(t)$	No. of requests dispatched from $Q_j^{(m)}$ to data center i at t
$s_j^{(m)}(t)$	No. of requests dispatched from $Q_j^{(m)}$ to private cloud at t

we assume that the video is always copied from the private cloud to the destination data center.

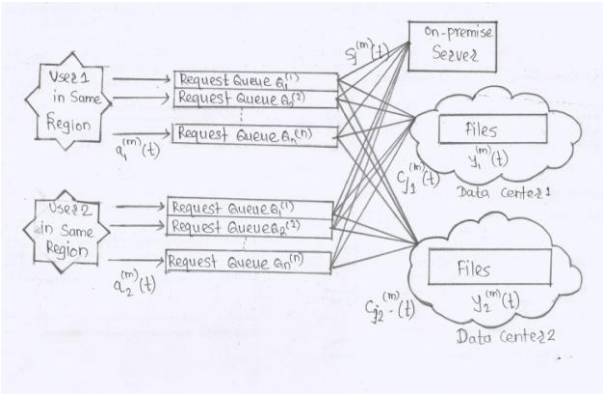

Fig2: Queuing Model

(2) For dispatching requests from region j for file m, let $s_j^{(m)}(t)$ be the number of requests to be served by the private cloud in time slot t, and $c_{ji}^{(m)}(t)$ denote the number of requests dispatched to data center i in time slot t, with an upper bound of μmax. Based on the elasticity of clouds, we reasonably assume that Amax < μmax. Requests for file m can only be dispatched to data center i when it stores the file, i.e., $c_{ji}^{(m)}(t) > 0$ only if $y_i^{(m)}(t) = 1$. We assume that a data center can serve a file to users in the time slot when the file is being copied to the data center, since replicating the file from the private cloud and serving chunks of the file can be carried out in parallel: after receiving a small portion of the file, a data center can already start to serve the received chunks of the file to users. We assume that upload bandwidth is reserved for replicating files to data centers from the private cloud, and this bandwidth is not counted in b, the maximum units of bandwidth that the private cloud can use to upload contents to users.

Operational cost. Our algorithm focuses on minimizing recurring operational cost of the content distribution system, not one-time costs such as the purchase of machines in the private cloud and contents. The recurring costs in each time slot t include the following categories: i) Bandwidth charge at the private cloud for uploading contents to users.
ii) Storage cost at data center iii)Request service cost at data center. iv) Migration cost for copying files from the private cloud to data center i.

4.1 Control algorithm on control center

Initialization: Set up request queue $Q_j^{(m)}$, virtual queues G and $Z_j^{(m)}$,∀j ∈ N, m ∈M, and initialize their backlogs to 0;

In every time slot t:

1. Enqueue received requests to request queues ($Q_j^{(m)}$'s);
2. Solve optimization Eq. (1)

$$\max \quad F(t) = \sum_{m\in\mathcal{M}}\sum_{j\in\mathcal{N}} s_j^{(m)}(t)\gamma_j^{(m)}(t) + \sum_{m\in\mathcal{M}}\sum_{j\in\mathcal{N}}\sum_{i\in\mathcal{N}} c_{ji}^{(m)}(t)\eta_{ji}^{(m)}(t) - \sum_{m\in\mathcal{M}}\sum_{i\in\mathcal{N}} \phi_i^{(m)}(t)y_i^{(m)}(t)$$

….(1)

This equation is to obtain optimal content placement and load distribution strategies $c_{ji}^{(m)}(t)$, $s_j^{(m)}(t)$, $y_i^{(m)}(t)$, ∀j,i ∈N,m ∈M;

3. Update content placement table with y(m) i (t)'s, and migrate files as follows:

for i ∈ N, m ∈ M do
if $y_j^{(m)}(t-1) = 0$ and $y_j^{(m)}(t) = 1$ then
Instruct data center i to request file m from private cloud;
if $y_j^{(m)}(t-1) = 1$ and $y_j^{(m)}(t) = 0$ then
Signal data center i to remove file m;

4. Dispatch $s_j^{(m)}(t)$ requests from queue $Q_j^{(m)}$ to private cloud, $c_{ji}^{(m)}(t)$ requests to data center i, ∀j,i ∈N,m ∈M; 5. Update virtual queue $Z_{ji}^{(m)}$ and G according to following equations (2) and (3);

$$Z_j^{(m)}(t+1) = \max[Z_j^{(m)}(t) + 1_{\{Q_j^{(m)}(t)>0\}}(\epsilon_j^{(m)} - s_j^{(m)}(t) - \sum_{i\in\mathcal{N}} c_{ji}^{(m)}(t)) - 1_{\{Q_j^{(m)}(t)=0\}}\mu_{max}, 0], \quad (2)$$

$$G(t+1) = \max[G(t) + \sum_{j\in\mathcal{N}}\sum_{m\in\mathcal{M}}(s_j^{(m)}(t)d_j + \sum_{i\in\mathcal{N}} c_{ji}^{(m)}(t)e_{ji}) - \alpha\sum_{j\in\mathcal{N}}\sum_{m\in\mathcal{M}}(s_j^{(m)}(t) + \sum_{i\in\mathcal{N}} c_{ji}^{(m)}(t)), 0]. \quad \ldots.(3)$$

5. AES ALGORITHM

To providing security to the data is always having a importance issue because of the critical nature of the cloud and very large amount of complicated data it carries, the need is even important. Therefore, data security and privacy issues that need to be solved have they are acting as a major obstacle in adopting cloud computing services [1].

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

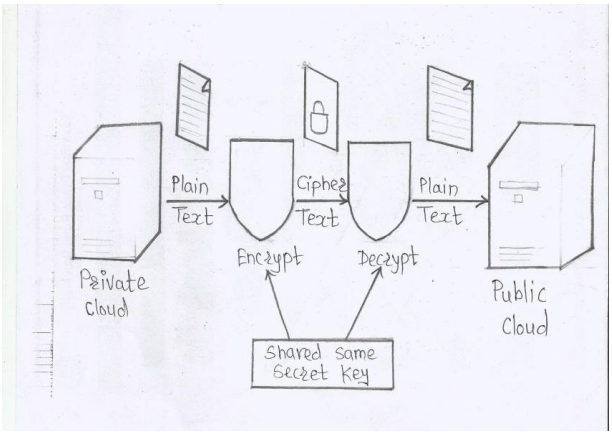

Fig 3: AES Basic Architecture

The main security issues of cloud are:
1. Privacy and confidentiality Once cloud outsources data over the cloud there should be some guarantee that data is accessible only to the authorized user. The cloud user should be confident that data stored on the cloud will be confidential [1].
2. Security and data integrity Data security can be provided using different encryption and decryption techniques. With providing security to data, cloud service provider should also implement technique to monitor integrity of data on the cloud [1].
These are the algorithms which are used for encryption and decryption:
Symmetric Algorithms:
DES: Data Encryption Standard (DES) was developed in year 1977 by National Institute of Standards and Technology (NIST). Key size for DES is 64-bits with block size 64-bits. Since 1977, too many attacks and methods have witnessed DES problems which made it as insecure block cipher [1].
3DES: This was developed in year 1998 as an improvement of DES. In 3DES standard similar to the original DES but it applied three times encryption level. So, 3DES encryption is slower than other encryption block cipher 26 2015 IEEE International Advance Computing Conference (IACCmethods. It has 64- bits of block size and 192-bits of key size. 3DES has low performance in terms of power consumption and throughput and it requires more time to encrypt than DES because of triple phase encryption.
AES: The AES (Advanced Encryption Standard) is the new best encryption algorithm by NIST to replace DES. It is a symmetric-key block cipher algorithm. The AES algorithm has 3 fixed 128-bit block ciphers with cryptographic keys i.e. 128 bits, 192 bits and 256 bits. The size of key is unlimited, where the block size is maximum 256 bits. AES encryption technique is fastest, flexible and secured. It can be supported on various platforms i.e. in small devices.

2. Asymmetric Algorithms:
RSA: This is a best Internet encryption, decryption and authentication system which is developed in year 1977 by Rivest, Shamir, and Adleman. RSA algorithm is the most used encryption technique. It is the only algorithm which is used for public key cryptography. It is a fastest encryption technique.

5.1 Algorithm: Description of the AES Encryption algorithm:
1. Key expansion – From key schedules derives round key from its ciphers.
2. Initial round – a. Add round key – by using bitwise XOR combine each bit with round key.
3. Rounds – a. Sub bytes – each byte is replaced with another byte using
a look-up table as a non-linear substitution.
b. Shift rows – each row is shifted cyclically to a number of times called transposition.
c. Mix the columns – combines four bytes in each column.
d. Add round key 4. Final round – a. Sub bytes b. Shift rows c. Add round key
II. Encryption algorithm:
1) Inverse shift rows
2) Inverse substitute bytes
3) Add round key- step consists of XORing the output of the previous two steps
4) Inverse mix columns

6. CONCLUSION

This paper concludes, optimal migration of a content distribution service to a hybrid cloud. Which minimizes the operational cost of the application with QoS guarantees. This paper also helps to deal with security issue using AES algorithm while content migration.

REFERENCES

[1] Amazon CloudFront, http://aws.amazon.com/cloudfront/.
[2] Microsoft Azure, http://www.microsoft.com/windowsazure/.
[3] Google App Engine, http://code.google.com/appengine/.
[4] M. Hajjat, X. Sun, Y. E. Sung, D. Maltz, and S. Rao, "Cloudward Bound: Planning for Beneficial Migration of Enterprise Applications to the Cloud," in Proc. of IEEE SIGCOMM, August 2010..
[5] M. J. Neely and L. Golubchik, "Utility Optimization for Dynamic Peer-to-Peer Networks with Tit-For-Tat Constraints," in Proc. of IEEE INFOCOM, April 2011..
[6] S. T. Maguluri, R. Srikant, and L. Ying, "Stochastic Models of Load Balancing and Scheduling in Cloud Computing Clusters," in Proc. of IEEE INFOCOM, 2012.
[7] Xuanjia Qiu , Hongxing Li , Chuan Wu Zongpeng Li and Francis C.M. Lau," Cost-Minimizing Dynamic Migration of Content Distribution Services int Hybrid Clouds",in2015.
[8] Mr. Niteen Surv, Mr. Balu Wanve, Mr. Rahul Kamble, Mr. Sachin Patil , Mrs. Jayshree Katti "Framework for Client Side AES Encryption Technique in Cloud Computing".