DEPLOYING VIRTUAL DATA CENTER ON CLOUD PLATFORM

[1]Nayan Tulsidasbhai Patel, [2]Girish Khilari
[1]PG Student, [2]Chair - Industry Relations – IEEE Pune Section,
[1]Department of Computer Engineering,
[1]GTU PG SCHOOL, Gandhinagar,Gujarat, India

***Abstract*—A data center is a facility that centralizes an organization's IT operations and equipment, and where it stores, manages, and disseminates its data. Data centers house a network's most critical systems and are vital to the continuity of daily operations.**
Initial and Operation cost of data center is very high. Expansion of storage capacity of data center is very difficult.
On the other hand, public clouds are less expensive compare to data center. Also operation cost is low as the up time is maintained by service provider as per Service Level Agreement.
We introduce a protocol to connect public clouds to create virtual data center. The virtual data center is a method of dynamically allocating resource. It is very easy to expand the storage capacity of in virtual data center as we have to just connect more clouds.

IndexTerms— Virtual Data center, cloud computing, resource allocation

I. CLOUD COMPUTING

Cloud Computing is a general term used to describe a new class of network based computing that takes place over the Internet, a collection/group of integrated and networked hardware, software and Internet infrastructure. And Using the Internet for communication and transport provides hardware, software and networking services to clients. These platforms hide the complexity and details of the underlying infrastructure from users and applications by providing very simple graphical interface or API (Applications Programming Interface).Cloud Computing has following Deployment Models:

A. PUBLIC CLOUD

A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud services may be free. Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services that are made available by a service provider for a public audience and when communication is effected over a non-trusted network.

B. PRIVATE CLOUD

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally. Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment, and requires the organization to reevaluate decisions about existing resources. When done right, it can improve business, but every step in the project raises security issues that must be addressed to prevent serious vulnerabilities.

C. HYBRID CLOUD

Hybrid cloud is a composition of two or more clouds that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.Varied use cases for hybrid cloud composition exist. Hybrid cloud adoption depends on a number of factors such as data security and compliance requirements, level of control needed over data, and the applications an organization uses.

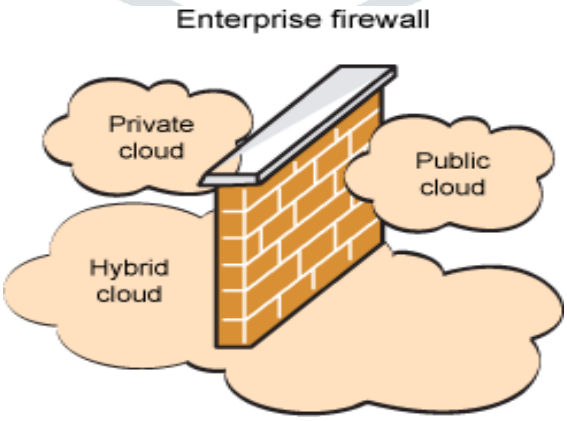


Figure 1.1 Types Of Cloud Based on Deployment

II. VIRTUAL DATA CENTER

A Virtual Datacenter is a pool of cloud infrastructure resources designed specifically for enterprise business needs. Those resources include compute, memory, storage and bandwidth.Virtual Data Center offers a pool of virtual resources. Customer can use it to create own IT infrastructure for any complexity level, creating virtual structure, which functions are completely similar to physical equipment solutions. VDC service is based on Infrastructure as a Service model (IaaS).Virtual Data Center Service (VDCS) is a managed, on-demand service that achieves true enterprise computing in a cloud-based environment, think of it as your virtual data center in a shared cloud.The virtual data center is a method of dynamically allocating resource.

III. HOW TO SECURE VIRTUAL DATA CENTER

To secure the virtual data center we have to secure the public clouds. For that we secure the access to public cloud. And also the security of data is very important. Data should not be reviled to someone else other that the authorized user. Also no other than authorized user can store data to virtual data center.

Also data should be secure while it is in transits. Data received must be same as data sent by sender. No one can modify data while data is in transits. Also no one can pretend to be sender. Means no one can fabricate the data or read or write request.

So to ensure the security of virtual data center we have to secure the access to clouds where data actually stores and also security of data is very important. We have to ensure data integrity, too.

IV. PROPOSED MODEL

Proposed The Model of Virtual Data Centre That Consist Following Modules:

- Subscribers
- Controllers
- Public clouds

A. SUBSCRIBERS

Subscriber in proposed virtual data center is the clients of service.

It Consist of following:

- Subscriber information
  - Subscriber information is the identity of client. It consists of following data.
  - ID
  - Secret Key
- User groups

  Subscriber can create and remove user group within its subscriber id. It is like user groups in unix file system.

  It is used to give access permissions on file.
- Users

  Subscriber can create users in any user groups. It is like users in unix file system.

  It is used to give access permissions on file.
- Encryptions
  - Here in proposed virtual data center subscribers are independent to define and use any encryption technique they want to use. For this they only add algorithm technique in following structure:
  - Enc_id
  - Algorithm
  - Key

B. CONTROLLERS

Controllers are servers that are used to manage data in public clouds connected with it by VPN.

They are managing following information:

- Subscribers

  This consists of list of subscribers and their secret key. This is like the list of clients, it is hosting.
- Clouds

  This consists of the list of followings information of public clouds connected to it by VPN.
  - Ip / hostname
  - description
- Data

  This is the list of data of any of its subscriber. Data is not actually on the controllers, it stored on public clouds attached to it. This list is only used for keep track of data.

  This consist of following fields:
  - Subscriber
  - User group
  - Username
  - Permission
  - Virtual path
  - Cloud ip
  - Real path

C. ARCHITECTURE

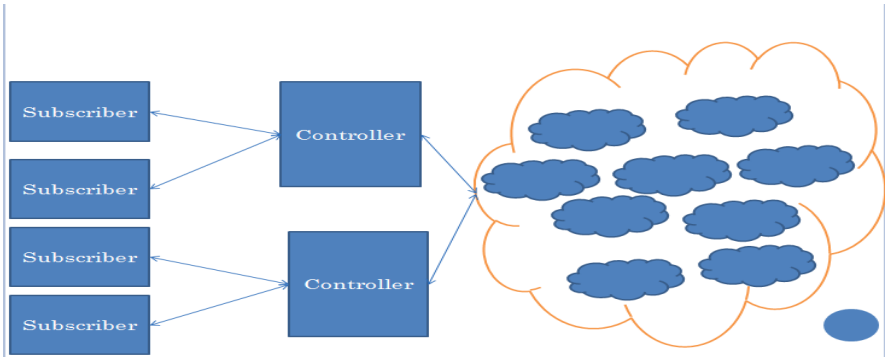


Figure 6.1 Virtual Data Center – Architecture

The figure above shows the architecture of proposed virtual data center. Here as shown one or more subscribers are connected to a controller; and each controller is connected to many public clouds.

Here first data is divided in to the blocks of any size randomly. Sequence no. of each block is attached to that data block in the starting and hash of data is attached in the end of it. Here we use SHA-3-512 for hashing.

Now we can process all the data blocks in parallel. Now data is encrypted by selected encryption algorithm, and Enc_id of it is attached to it.It is connected with the Control Label. Control label is encrypted by shared secret key of subscriber. It is decrypted at controlled to keep track of data.Controller reads Control label and add Data Record. Then select best public cloud to store it.

V. THE WORKING OF VIRTUAL DATA CENTER

The Virtual Data Center Works by Protocol Defined over Existing Public Cloud Protocol Stack. This Protocol Defines three operations of virtual data center.Uploading the data to virtual data center, downloading data from virtual data center and deleting the data from virtual data center are three operations defines in protocol.

A. UPLOADING DATA TO VIRTUAL DATA CENTER

To upload data to virtual data center client forward data to controller and then controller stores metadata and forward this data to public clouds. The operation is described below.

- Client
  1. Split Data in Variable Size Chunks
  2. Append Sequence no. as header and hash as Trailer
  3. Generate control label and encrypt by secret key shared with controller that is same for all chunks
  4. Append length of control label encrypted by secret key shared with controller and append
  5. Process all chunks in parallel manner
     1. Encrypt chunks along with sequence and hash
     2. Append previously generated control label to payload
     3. Encrypt its subscriber id by public key of controller and append it to pay load
     4. Send this to controller
- Controller
  1. Receive packet created by client.
  2. Decrypt subscriber id by its private key
  3. Decrypt length of pay load by shared secret key of that subscriber
  4. Decrypt control label with by shared secret key of that subscriber
  5. Check if subscriber id from control label and decrypted by its private key is same or not?
     1. If not same, this is Fabricated payloads, Discard it
     2. If same, store Metadata and forward data to public cloud

The figure below is divided in to two parts. Left part shows data dived in to variable sized chunks and encrypted, etc as described before. And right part describes the control label.

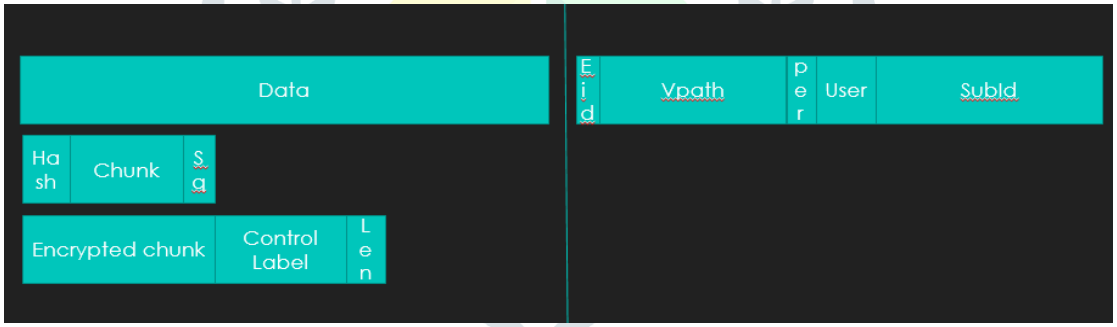


Figure 7.1 Control Label and Encrypted payload for upload

B. DOWNLOADING DATA FROM VIRTUAL DATA CENTER

To download the data, client creates a GET request label and send to controller and then controller and controller and client creates one-time links and submit to client. It acts as a ticket. The operation is described below.

1. Subscriber id encrypted with public key of controller is generated
2. Get Request is generated and previous payload is append to it
3. Calculate Length of Request and encrypt it by secret key shared with controller and append to request
4. Check if subscriber id in Get Request Packet and Encrypted by its public key is same or not
5. If not same, it is fabricated request, discard it
6. If same then forward this request to cloud where data actually stores and get request URI From Cloud and Forward it to Client. This URI Acts as Ticket and can be uses one time only
7. Client get All chunks by URIs. And Decrypt them in parallel
8. Now by reading sequence no and calculate and match hash and combine accordingly.

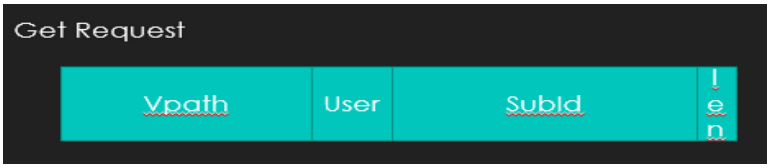


Figure 7.2 Get Request for Download Operation

C. DELETING THE DATA FROM CENTER

To Delete the data client generates delete request and forward to controllers, the controller reads all data block information and forward the request to delete them to clouds. The structure of the delete request is exactly the same as Get Request. Steps of delete operations are as below.

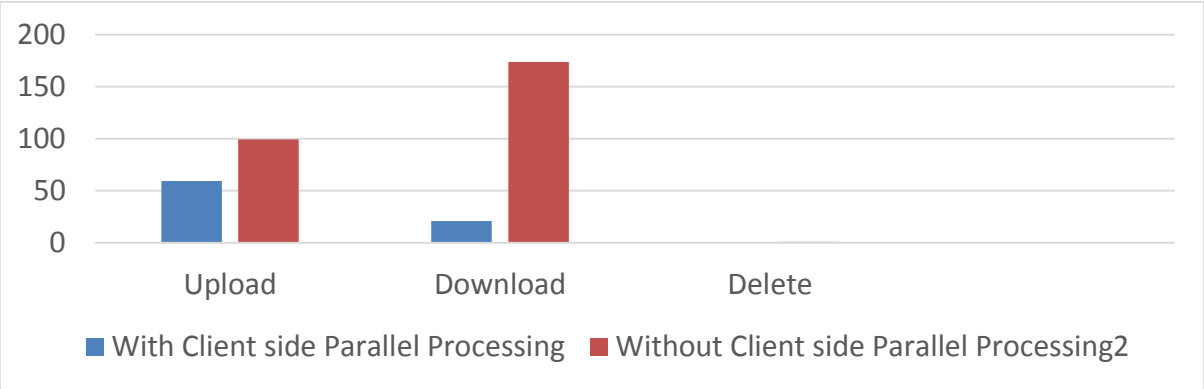
- Client send same Request as Get Request
- Controller Read information about all chunks and forward to clouds they actually holds the data.
- Cloud Delete Those Data.

VI. RESULT COMPARISON OF OPERATIONS WITH CLIENT SIDE PARALLEL PROCESSING AND WITHOUT IT

Following table and graph show the result comparison of operations with client side parallel processing and without client side parallel processing.

Round time for / by	upload	download	delete
Client Side Encryption of all chunks in parallel	59.37	20.84	0.56
Without it	99.41	173.65	0.74

Table 9.1 Result Comparison of operations with client side parallel processing and without it



VII. SECURITY ASPECTS

Security attacks are classified as interception attacks, modification attacks and fabrication attacks.

Interception attacks on our proposed virtual data center is difficult as users uses different encryption algorithms and can change it anytime. And control information is also encrypted by shared secret key that is shared between client and controller only.Modification attack is also difficult on our proposed virtual data center as data is divided in to variable size blocks and each block has SHA 256 hash value attached to it in encrypted form.

Fabrication attack is also difficult in out virtual data center as first subscriber id is sent to controller by encryption it by public key of controller. And control labels also have subscriber id encrypted by secret key, if they do not match fabrication attack detected and mitigated.

VIII. CONCLUSION

We can create secure virtual data center service by proposed scheme. We can dynamically allocate the resources i.e public clouds for on demand scaling of virtual data center service. The virtual data center is more flexible in data management and takes less cost to provide service. The cloud user feels more secure to put his data onto the data center.

REFERENCES

[1] Huan Zhou, JiangchunRen, "A Secure Virtual Data Center Based on Data Labeled Cloud-agent", Software Engineering and Service Science (ICSESS), 2014 5th IEEE International Conference, pp 937 - 940.

[2] Mohan, Devi Priya V S, "An improved approach for Enhancing Public Cloud Data Security through Steganographic Technique", International Conference on Inventive Computation Technologies (ICICT 2016).

[3] Frederic Francois, ErolGelenbe, "Optimizing Secure SDN-enabled Inter-Data Centre Overlay Networks through Cognitive Routing", IEEE MASCOTS 2016, At Imperial College, London.

[4] Max Alaluna, Fernando M. V. Ramos, NunoNeves, "(Literally) above the clouds: virtualizing the network over multiple clouds", 2016 IEEE NetSoft Conference and Workshops (NetSoft), pp 112 - 115.

[5] Micah Altman, L. Andreev, M. Diggory, G. King, E. Kolster, A. Sone, S. Verba, "Overview of The Virtual Data Center Project and Software", The First ACM+IEEE Joint Conference on Digital Libraries.

[6] Ahmed Amokrane, Mohamed FatenZhani, Rami Langar, RaoufBoutaba, Guy Pujolle, "Greenhead: Virtual Data Center Embedding across Distributed Infrastructures", IEEE Transactions on Cloud Computing 2013, pp 36-49.

[7] Qi Zhang, Mohamed FatenZhani, MaissaJabri, RaoufBoutaba, "Venice: Reliable virtual data center embedding in clouds", IEEE INFOCOM 2014 - IEEE Conference on Computer Communications 2014, pp 289 - 297