An Empirical Performance Study of Secured Virtual Machine Migration for Inter-Cloud Networks

Akika Yamashita
Ochanomizu University
Department of Computer Sciences
Email: akika@ogl.is.ocha.ac.jp

Eng Keong Lua
MONASH University
Faculty of Information Technology
Email: eklua@computer.org

Masato Oguchi
Ochanomizu University
Department of Computer Sciences
Email: oguchi@computer.org

***Abstract*—In recent years, big data are managed by Cloud instead of local environment such as users' own devices. There are a lot of advantages of managing big data on Cloud, However, Cloud computing technology has demerits that cannot be ignored — Security. For example, the operating system (OS) on the host server is managing all VM, thus, if the host server are compromised, the important data and information of users will be lost and stolen. Migration must be executed securely especially on inter-Cloud, and the VMs must be migrated through safe and secure network such as security architecture for Internet Protocol (IPsec). However, there is trade-off between security and speed of migration. Stronger security mechanism makes the migration speed slower. For example, IPsec is not efficient and takes much longer time to complete the migration. In this paper, we have proposed a method to execute Cloud migration securely and quickly. Our method is based on the intuition on optimization efficiency to execute encryption and decryption to increase the speed of migration. In our method, we have encrypted all VM on source Cloud (server) before migration, send the VM to another Cloud (server) through the network, and decrypt the VM at the destination Cloud (server). Our realistic comparison results showed dramatic performance improvement. We are planning to use this promising research results to examine (1) speed of encryption (2) partial encryption, as our future research work.**

I. Introduction

In recent years, the data on real-world and cyber-space have increased dramatically due to the recent development of data collection and analytic technologies as well as high diffusion of Social Networking Service (SNS). As a result, these big data are managed by Cloud instead of local environment such as users' own devices. The advantages of managing big data on Cloud are as follows: (1) users do not need to possess large storage capacity or dedicated data management software, (2) users can access required data through wired or wireless networks and by any devices such as personal computers (PC) or Smart phones or tablet devices, (3) the virtual machine (VM) on Cloud can be replicated and migrated to another server for disaster recovery seamlessly.

Cloud-computing technology has evolved from ”single-Cloud” (composed of private cloud and public cloud separately) to ”hybrid Cloud” (composed of private cloud and public cloud connected with network), and then to near future ”inter-Cloud” (composed of several clouds connected with network). However, Cloud computing technology has demerits that cannot be ignored — Security. For example, user cannot access their own data or VM physically when the VM is optimally migrated to another server. In addition the operating system (OS) on the host server is managing all VM, thus, if the host server are compromised, the important data and information of users will be lost and stolen.

Migration must be executed securely especially on inter-Cloud because different data and VM will be migrated to another cloud not just another host. The VMs must be migrated through safe and secure network such as security architecture for Internet Protocol (IPsec). However, there is trade-off between security and speed of migration. Stronger security mechanism makes the migration speed slower. Especially in IPsec, the whole data is divided to small fragments and encryption is applied to each fragment. As a result, big-sized VM will take much longer time to complete the migration. This is not efficient.

In this paper, we have proposed a method to execute Cloud migration securely and quickly. Our method is based on the intuition on optimization efficiency to execute encryption and decryption to increase the speed of migration. In our method, we have encrypted all VM on source Cloud (server) before migration, send the VM to another Cloud (server) through the network, and decrypt the VM at the destination Cloud (server). We compared our method with existing migration technique using IPsec tunnel. Our realistic comparison results showed dramatic performance improvement. We are planning to use this promising research results to examine (1) speed of encryption (2) partial encryption, as our future research work.

Outline. We explain the characteristics of migration on inter-Cloud in section II and describe our experimental environment in section III. We show the comparison results of our experiments in section IV. We further discuss the effectiveness of our experiment in section V. Finally, we conclude this paper in section VI.

II. Inter-Cloud

A. The Composition of Inter-cloud

As discussed above, the inter-cloud is an extension of single-cloud and hybrid-cloud. The evolution of cloud computing is shown in Fig. 1. In single cloud, private cloud and public cloud exists separately. Private cloud is used by some companies or personal users with private internal network. Public cloud is managed by cloud providers such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) providers. User who want to use public cloud have to contract and pay for a cloud provider service. In hybrid cloud, private cloud and public is connected

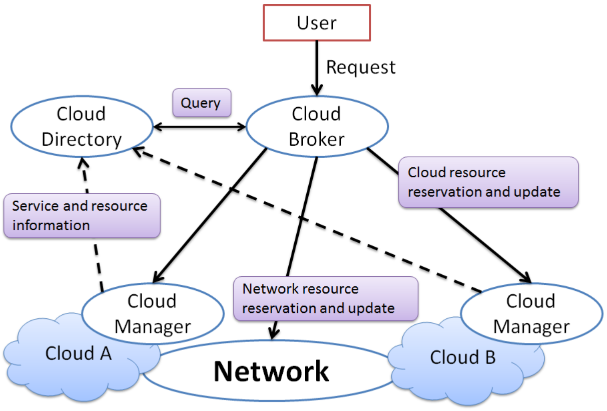
User
Request
Query
Cloud Directory
Cloud Broker
Service and resource information
Cloud resource reservation and update
Network resource reservation and update
Cloud Manager
Cloud Manager
Cloud A
Network
Cloud B

Fig. 2. The architecture of Inter-cloud

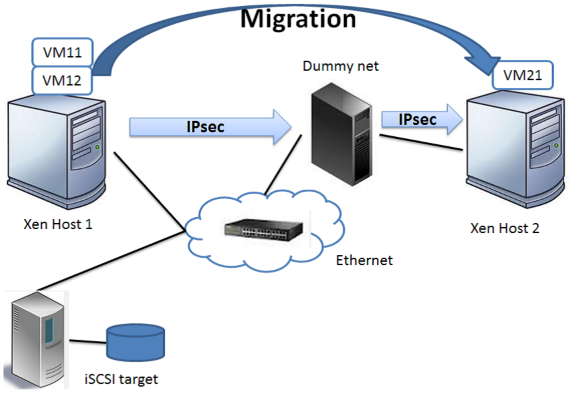

Fig. 3. Supposed migration on inter-cloud

with network, and the data and information on private cloud can be seen or used by public cloud at least temporarily. Though the data and information of each contractor can not be seen from each other, the network connection must be secure. In inter-cloud, private cloud and public cloud of different cloud providers are connected with same network, thus, the security should be even more strong.

The architecture of Inter-Cloud is shown in Fig. 2. Inter-cloud is managed by cloud broker, cloud manager, and cloud directory. Cloud broker receives the request of resource reservation from users and selects proper cloud and send the request of resource reservation to the cloud and network. Cloud manager manages each cloud resources and executes accounting, allocation. Cloud directory collects information of cloud service and resources from cloud manager, and corresponds to the query of proper cloud service.

B. Characteristic of Migration on Inter-cloud

Inter-cloud technology allows different types of cloud connected with network — inter-cloud. In addition, VM and data migration can be executed through different types of cloud which managed by different cloud providers. Thus, when a server host crashes or wide-scale disaster happens, inter-cloud technology can protect users data, information and lifeline safely with sharing the resources among different cloud. Additionally, with migrating VM optimally to the nearer server of users, users can use their resources without being aware of delay.

As for the network for migration on inter-cloud, the secure network such as IPsec is supposed to be used. As shown in the Fig. 3, the existing migration on inter-cloud are supposed to be as follows : (1)shutdown the VM of host server on a cloud, (2)migrate the VM another cloud through IPsec tunnel, (3)restart the VM on destination server on the other cloud. While migrating the VM through IPsec tunnel, the data will be separated into small part on IP layer and each IP layer packet will be encrypted each time. Though the security is strong, IPsec is not so efficient. In addition, there is another way of migration — live migration in which shutdown and restart of VM are not necessary. In live migration using IPsec, the existing method is supposed to take much time as the process is complex. In IPsec, the packet of IP layer is encrypted and safely transmitted. The sender side and receiver side decide the key based on Security Association (SA), and Internet Key Exchange (IKE) is used on receiver side authorization. In this paper, we only executed the experiment of migration, live migration will be future work.

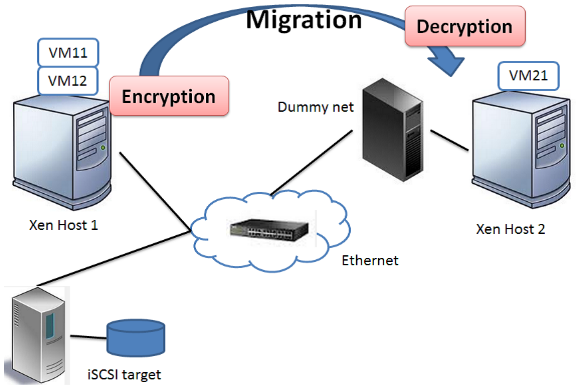

Fig. 4. Our proposed migration on inter-cloud

In this paper, we suggest that encryption and decryption on each IP packet very inefficient. As shown in the Fig. 4, our proposed way is as follows:

1) Shutdown the VM on sender side
2) Encrypt all the VM
3) Send VM with Secure Copy protocol (SCP)
4) Decrypt all the VM on receiver side
5) Restart the VM on receiver side

In the experiment of this paper, we have shown that our proposed method is much better than existing method especially on high-latency environment. The detail of experiment result is discussed in section IV.

III. Experimental Environment

We have compared performance of following two methods: (1) migration using IPsec tunnel (Fig. 3), (2) our proposed migration method (Fig. 4). The real terminal experiment have been executed with two nodes supposed to belong to two different clouds.

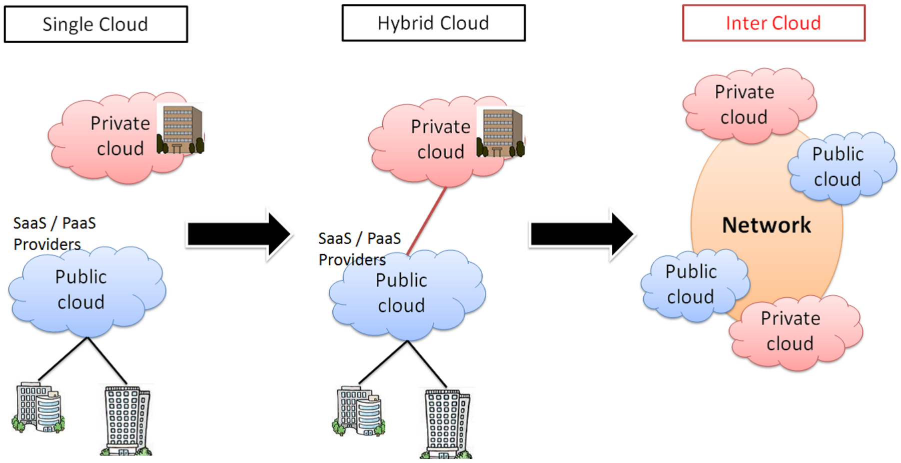

Fig. 1. Evolution of cloud computing

A. Terminal in the experiment

We have installed Xen [1] as virtual machine monitor on each host server. Xen provides a service of parallel processing and control of multi operating system (OS) with one hardware. In xen, each VM is called ”domain”. Xen hypervisor supports one or several OS and executes scheduling to physical Central Processing Unit (CPU). The host OS is called Domain-0 (dom0) and newly added OS (VMs) are called Domain-U(domU). On each host server, one dom0 manages several VM, domU. Dom0 starts automatically after hypervisor is booted and management authority is given. Every physical hardware can be accessed from dom0 directly. System administrator can login to all domU from dom0.

We have used iSCSI [2] as data storage for two xen host servers. iSCSI is a protocol to use SCSI protocol on TCT/IP network. It is standardized on transport layer. Recently, SAN storage is composed with Fiber Channel, however, the cost of establishing a network of Fiber channel is high. iSCSI is a technique to compose SAN, but iSCSI can be used with TCP/IP network instead of fiber channel. We have settled one iSCSI target which is storage server and iSCSI initiator which is client to access iSCSI target. In our experimental environment, iSCSI initiator is installed to dom0 on each xen host server.

We have sandwiched dummynet between Xen host 1 and Xen host 2, in other word, source server and destination server of migration. Dummynet is used to make high latency environment artificially. The spec of each terminal in the experiment is shown in TABLE. I, II, III, and IV.

When migrating the VM through IPsec tunnel, we have run IPsec with installing openswan package [3]. Xen host 1 (source terminal of migration) is IPsec client, and Xen host 2 (destination terminal of migration) is IPsec server. In our proposed method, we have executed encryption and decryption with openSSL [4].

B. Command Line in the Experiment

1) Migration through IPsec tunnel:

1) Start iSCSI target

TABLE I. Xen host server 1 and 2 (same spec)

OS	Linux 2.6.32-5-xen-amd64 and xen-4.0-amd64
Distribution	Debian GNU / Linux 6.0.2
CPU	Intel(R) Xeon(R) CPU 3.60GHz
Memory	4 GByte
Disk	222 GByte

TABLE II. VM and iSCSI initiator on Xen host server 1 and 2 (same spec)

OS	Linux 2.6.32-5-xen-amd64 and xen-4.0-amd64
Distribution	Debian GNU / Linux 6.0.2
CPU	Intel(R) Xeon(R) CPU 3.60GHz
VCPU	1 core
VCPU Memory	2 GByte
Storage	open-iscsi-2.0-873
Disk	5 GByte

TABLE III. iSCSI target

OS	Linux 2.6.32-5-amd64
Distribution	Debian GNU / Linux 6.0.2
CPU	Intel(R) Xeon(R) CPU 3.60GHz
Storage	open-iscsi-2.0-873
Disk	130 GByte

TABLE IV. Dummynet

OS	FreeBSD 6.4-RELEASE
CPU	Intel(R) Xeon(R) CPU 3.60GHz
Disk	64 GByte

2) Connect to iSCSI target from two iSCSI initiator (Xen host server 1 and 2)

3) Create and start VM (domU) on migration source terminal
(Xen host server 1)

4) Start IPsec tunnel on both Xen host server
(1024bit RSA key)

5) Migrate the VM (domU) from migration source terminal to destination terminal
(Xen host server 1 to 2)

2) Our Proposed Migration:

1) Start iSCSI target

2) Connect to iSCSI target from two iSCSI initiator
(Xen host server 1 and 2)

3) Create and start VM (domU) on migration source terminal
(Xen host server 1)

4) Shutdown the VM(domU) on migration source terminal
(Xen host server 1)

5) Encrypt all the VM(domU)
(root directory of domU)
(256bit AES key)

6) Send encrypted VM(domU) with Secure Copy protocol (SCP) from source terminal to destination terminal
(Xen host server 1 to 2)

7) Decrypt all the VM(domU) on migration destination terminal
(Xen host server 2)

8) Restart the VM(domU) on migration destination terminal
(Xen host server 2)

The types of Encryption key of IPsec and VM encryption is different in our experiment, and uniforming the keys will be future work.

IV. Experimental Result and Discussion

The result is shown in Fig. 5. The graph is comparison of existing migration method (IPsec tunnel migration) and our proposed method. The vertical axis is time to complete VM migration and the unit is minute. The horizontal axis is round trip time (RTT) and the unit is millisecond (ms). We have measured RTT value from 0 (ms) to 200 (ms). When considering migration between two different located server, the distance is supposed to be longer and network latency is higher as the VM will be migrated among servers all over the world. For example, the distance from Tokyo, Japan to Osaka, Japan is about 550 km and RTT is about 20 ms. The RTT is about 120 ms from Tokyo, Japan to west part of United states, about 200 ms and more to Europe countries.

As shown in the graph in Fig. 5, The migration of domU took about 3.5 minutes (min) even though in no-latency environment and as the RTT increases, the migration time grows dramatically and migration took over eight minutes when the RTT is over 100 ms. IPsec is bottleneck of migration because the packet is divided into small segments, in addition, CPU allocation also makes migration time longer.

On the other hand, our proposed method performs well and migration time does not increase so much as RTT increases. The migration time is kept between 5 min and 6 min. In our proposed method, the bottleneck of migration time is encryption and decryption time of VM which is shown in Fig. 6. The graph in Fig. 6 shows the constant time of our proposed method. Each bar graph shows the time of Encryption time before migration, decryption time after migration, the total time of encryption and decryption, VM shutdown time before migration, VM restart time after migration, and total time of shutdown and restart of VM. As the graph shows, total time of encryption and decryption is about 5 min.

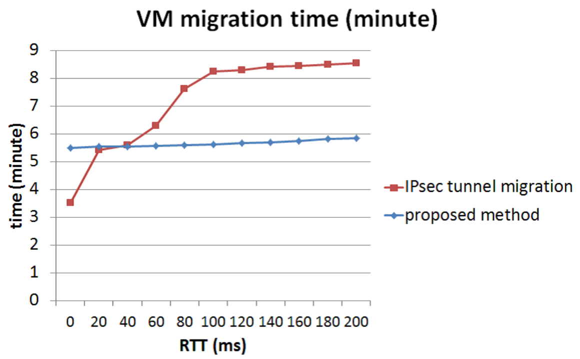

Fig. 5. Comparison of existing migration method and our proposed method

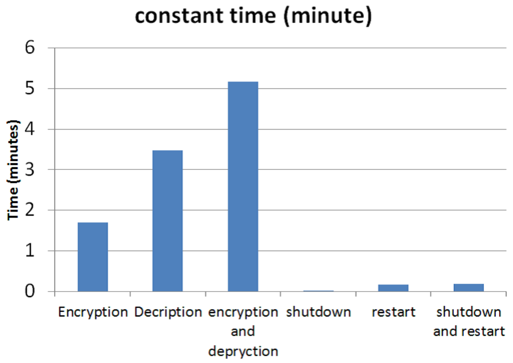

Fig. 6. Constant value on our proposed method

As the graph in Fig. 5 shows, when the RTT is 40 ms, the performance of two methods be almost same, and when RTT is over 60 ms, our proposed method performs better than existing method. An shown in Fig. 7, when the RTT is over 100 ms, the time of proposed method is about 60% of existing method. Our proposed method have achieved 40% performance improvement.

In the experiment in this paper, the encryption key type of existing method with IPsec tunnel(1024bit RSA key) and proposed method (256bit AES key) is different. We will uniform the key length and key type in future work. If the key type is changed, the cross point of graph shown in Fig. 5 is supposed to move. Stronger and longer key makes the graph of proposed method move to up. With improving speed of encryption and partial encryption, our proposed method can be improved more.

V. Related Work

Research in the area of VM migration mainly focused on optimizing migration performance through live migration. The mechanism of live migration which is a migration that not to stop VM before and after the migration is explained in [5] and mechanism is explained in [6]. In [7], the scalability of application services on Inter-Cloud is discussed. In [8], the technology that enables live mobility of VM on Inter-cloud is discussed but privacy and security is required. [9] and [10] is also discussing migration performance improvement.

As for the security consideration, J. Rexford et. al have

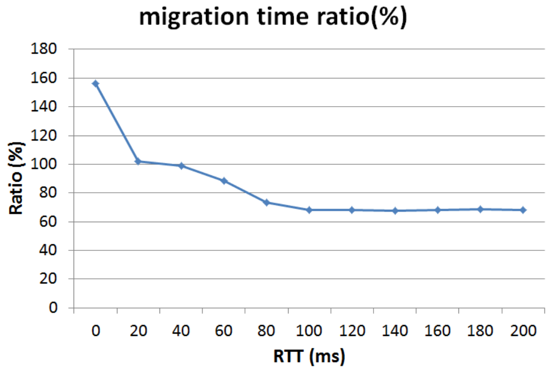

Fig. 7. The time ratio of proposed method to existing method

come out with no hypervisor. Securing hypervisor architecture is one of the good methods to achieve secure migration, but the method proposed is not sufficient as the vulnerabilities in current migration mechanisms. While the semantics and performance of live VM migration are well explored, the security aspects have received very little attention in an optimistic point of view, we are planning to develop a method that satisfies both characteristic - security and performance - paying attention to the trade-off between them. As for the security consideration, J. Rexford et. al have come out with no hypervisor. Securing hypervisor architecture is one of the good methods to achieve secure migration, but the method proposed is not sufficient as the vulnerabilities in current migration mechanisms. While the semantics and performance of live VM migration are well explored, the security aspects have received very little attention in an optimistic point of view, we are planning to develop a method that satisfies both characteristic - security and performance - paying attention to the trade-off between them.

VI. Conclusion

We have proposed new migration method and compared the performance of existing migration method using IPsec tunnel and our proposed method. In our proposed method, we do not use inefficient IPsec tunnel but execute encryption and decryption to all the VM before and after migration. Our proposed method in the realistic comparison results showed about 40% improvement in high latency environment such as 100 ms to 200 ms.

As the future work, we are planning to use this promising research results to examine (1) speed of encryption, (2) partial encryption to improve the migration performance of our proposed method as it is not necessary to encrypt all parts of VM. In addition, we will also consider live migration while we only treated ordinary migration in this paper.

References

[1] “Xen project,” http://xen.org/.

[2] “open-iscsi,” http://www.open-iscsi.org/.

[3] “Openswan,” https://www.openswan.org/projects/openswan/.

[4] J. Viega, M. Messier, and P. Chandra, “Openssl,” 2009, ”Network Security with OpenSSL”, O’Reilly.

[5] Diego Perez-Botero, “A brief tutorial on live virtual machine migration from a security perspective,” 2011, http://www.cs.princeton.edu/ diegop/courses.html.

[6] Jansen and Gerardus T., “Mechanism for inter-cloud live migration of virtualization systems,” 2012.

[7] R. Buyya, R. ranjan, and R. N. Calheiros, “Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services,” in *the 10th International Conference on Algorithms and Architecture for Parallel Processing (ICA3PP2010)*, May 2010, pp. 13 – 31.

[8] K. Nagin, D. Hadas, Z. Dubitzky, A. Glikson, I. Loy, and B. Rochwerger adn L. Schour, “Inter-cloud mobility of virtual machines,” in *the 4th Annual International Conference on Systems and Storage Article(SYSTOR2011)*, May 2011, p. No. 3.

[9] M. Tsugawa, P. Riteau, A. Matsunaga, and J. Fortes, “User-level virtual networking mechanisms to support virtual machine migration over multiple clouds,” in *IEEE GLOBECOM Workshops (GC Wkshps 2010)*, December 2010, pp. 568–572.

[10] Hong Xu and Baochun Li, “Egalitarian stable matching for vm migration in cloud computing,” in *IEEE INFOCOM Workshop on Cloud Computing(INFOCOM Workshop2011)*, 2011, pp. 631–636.