Security Migration Requirements: From Legacy System to Cloud and from Cloud to Cloud

Noor Ibrahim Hussein
College of Information Science and Engineering, Hunan University
Ministry of Higher Education and Scientific Research of Iraq, Changsha, 410082, China
noorabr82@yahoo.com

Mervat Hashem
College of Information Science and Engineering, Hunan University
Changsha, 410082, China
mervat@hnu.edu.cn

Zhiyong Li
College of Information Science and Engineering, Hunan University
Changsha, 410082, China
zhiyong.li@hnu.edu.cn

***Abstract*—Cloud computing became an emerging technology. The benefits have made a lot of institutions and companies looking to use this technology. The process of migration from legacy systems to cloud computing environments is a complex process. The migration process does not represent the movement of data, applications and service only but also presents the process from the early stages of planning and continue until after the selection and transfer of data to a specific deployment model.**

Security is the biggest concern to consumers during the migration process, whether immigration initial from legacy systems to the environment of cloud computing or migration between the clouds. This paper presents an overview of the security requirements: before, during and after the migration from legacy systems to cloud computing, as well as security requirements data migration between the clouds.

Keywords-Cloud systems; migration; cloud to cloud; cloud security

I. INTRODUCTION

Cloud computing became a hot topic these days many Individuals, enterprises and companies are looking for the benefits of this rapidly developing service. Cloud computing environments achieved an economies enhancement through the good use of resources specialization and efficiency. Cloud computing environments have three types: Private, Public, Community and Hybrid Cloud. National Institute of Standards and Technology (NIST) gave a good definition as a Deployment Models. We can illustrate them in a simple form as follows:

Public cloud: is the cloud environment that can be accessed by anyone. Infrastructure may be owned, managed and operated by a business, academic, or government organization, or some combination of them.

Private Cloud: the cloud environment can be accessed by only one organization this organization may contain many consumers. Infrastructure may be managed by the company itself or a third party, or a combination of them. Private cloud removes the fears about the customers' data security.

Community Cloud: the cloud can be used by a specific community of consumers from organizations that have common considerations. Infrastructure may be managed by one or more of those organizations in the community, a third party, or some combination of them.

Hybrid cloud: The cloud infrastructure is a combination of two or more cloud infrastructures (private, community, or public). The different infrastructures are bounded together by the standards that maintain data and application portability.

Many of references depended only on three types of the deployment models (Private, Public, and Hybrid Cloud). This is what we will adopt it in this paper. The service models are categorized in three models (SaaS, PaaS, and IaaS) as follows:

Software as a Service (SaaS): The consumer can use the provider's applications on the cloud infrastructure. The applications can be accessed from different customer devices through a web browser, or a program interface. The infrastructure cannot be handled by the consumer.

Platform as a Service (PaaS): The consumer can use tools supported by the provider (as programming languages, libraries, or services) to deploy onto the cloud infrastructure. The underlying cloud infrastructure cannot be managed or controlled by the consumers.

Infrastructure as a Service (IaaS): The consumer can use any computing resources for processing the network's services. The consumer can deploy and run random software that can include operating systems or applications. The infrastructure cannot be handled by the consumers but can be managed over the operating system.

The rest of this paper is structured as follows: the first part about cloud migration divided to two sections: migration from an organization's computers to the cloud and cloud-to-cloud migration, the second part: security requirement for those two kinds, third section: the conclusion.

II. CLOUD MIGRATION

Cloud migration is the process of moving data, applications or other business elements from an organization's computers to the cloud, Cloud migration includes moving data or other market components between cloud environments, which known as cloud-to-cloud migration. The manner of transitioning to a different cloud provider is identified as a cloud service migration. In any case, successful migration to a service provider's environment may require the use of middleware, such as a cloud integration tool, to bridge any gaps between the vendor's and the customer's technologies [2].

There are many tools to make the migration process as easy as possible. The vendors have tried to provide some tools to support decision making during the migration of IT systems to the cloud. Like using some tools to compare the cost of various cloud providers, deployment choice and usage scenarios and other tool which is a spreadsheet that determines the benefits and risk of using IaaS clouds from an enterprise perspective, it is an assessment for the risk as a starting point. No matter which tool is used since the data owner must ensure that data integrity and security are maintained during and after the migration. Both data integrity and security still a supreme authority on migration and its result [3,4]. Data owner must not only know benefits of cloud services, but also should know exactly what can migrate to the cloud and what should not.

A. Organization's computers to the cloud migration

Many companies seeking to migrate their systems and services, or part of them to the cloud, and this is not surprising the huge potential offered by cloud computing such as Unlimited Scalability, Reduced cost, Increased storage, Automation, Flexibility, Better mobility [5].

First, we have to define three essential terms in cloud migration; data migration, data integrity, and data security. Data migration: the term of migration implies a one-time transfer of any data to improve its standing resting position. Data integrity: The accuracy and consistency of stored data, data must be complete with no variations or compromises from the original. Data security: Every "chunk" of data has security features connected with it. The layer at which this data is accessed determines the characteristics that are applied to that layer. Furthermore, data security itself is like a layered cake, there is a security at every access level, and each layer is vital [3].

In a generic way, a data migration involves a process of transferring data from one location to another. This process means reading data from the source, performing an internal mapping of this data and then writing it to the target. This process usually occurs via an "engine". This engine can be of any form and can reside anywhere in the access stack.

The migration from traditional IT environments to the Cloud Computing Environment (CCE) can be complicated as evaluation the benefits, risks and costs.

The process of shifting all or part of an organization's data (data, applications and services) from on-site building beyond the firewall to the cloud, based on the (on-demand) where the information can be provided over the Internet. A simple model and supposition clarifying the types of migration and objectives use these different kinds of migration in Cloud Computing Environment (CCE) [6], as shown in Table I.

B. Cloud-to-cloud migration (C2C)

Cloud-to-cloud migration: Is the transfer of physical or virtual devices along with their associated configurations, operating systems, applications and storage from one cloud computing provider to another. Cloud-to-cloud migration allows an organization to change cloud computing providers without transferring data to in-house servers. Having the ability to pass easily between cloud providers is a significant concern when choosing a cloud provider. The cost of a cloud migration should not exceed the benefits of moving to a new cloud provider [7].

Enterprises or Institutions decide migrating data due to many reasons, such as cheaper price, or more secure service, may be service does not meet their needs, or to make backup in different cloud to their data to ensure from making data safe from any disaster, or to reduce the dominance of a single vendor on their data. This migration is between cloud storage systems. Another migration type is between clouds called workloads migration.

In cloud computing, the workload is the amount of processing that the source and target cloud environments, determine the workload migration complexity and cost. Table II explains the migration workloads type between clouds [8].

Another reason: that is inappropriate to invest money from some enterprises or organizations on hardware equipment. Although most of businesses and enterprises have their own private cloud; it is no longer sufficient for the growth of their data. Therefore, they decided to transfer their data to a public cloud. E.g., Social Networks like Facebook, Myspace, and Online Markets like eBay, Taobao [9].

TABLE I. MIGRATION TO THE CLOUD

Type of migration	what is transferred	Kind of movement	The objective of use the Cloud computing
Data migration	Data	Manual	To be processed by an available server using standard applications.
Information migration	Information + its own schema + processing request	Semiautomatic	Select the best location based on the processing requirements.
Service Migration	Applications (perhaps, along with data)	Manual to App. and Automatic to data	For processing, the applications transferred may be unique or proprietary to the organization.
Autonomic Migration	Data + Information + Applications	Automatic of Data, Information and Applications	User services and data reside somewhere in the cloud along with additional information about processing requirements.

We can expand the concept of a set of migration patterns in Table II, which span from legacy IT environment to the

cloud by adding two patterns. Migration from Traditional IT to Public Cloud and Traditional IT to Private Cloud [8].

III. SECURITY AND PRIVACY ISSUESS

In this section, we divided cloud migration security into three levels as shown in figure 1.

A. *Before data migration*

- Data security plan: The first question is "DO you have a data security plan in your data migration strategy?" While planning to the data migration, the user must take into account how to reduce the potential risks through efficient planning and scoping.

TABLE II. WORKLOAD TYPES OF CLOUD TO CLOUD MIGRATION

Migration from	Migration to	Movement
Private Cloud	Public Cloud	This type focuses on the movement of one or more workloads from the private to the public CCE
Private Cloud	Hybrid Cloud	This movement type contains the bidirectional movement of workloads between a public and private cloud computing.
Public Cloud	Private Cloud	This is an unusual movement. The workload movement and migration type support a performance testing screenplay in the public venue before moving back internally
Public Cloud	Public Cloud	Includes a migration and movement effort to lift and move a workload between two CCE, which are using the public delivery model like moving from Amazon EC2 to the IBMcloud or vice versa.

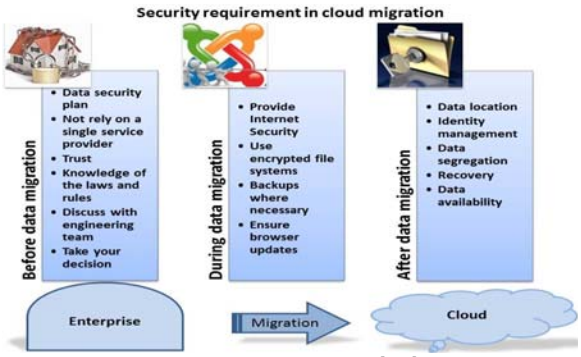

Figure 1 Security requirement in cloud migration

- Not rely on a single service provider: If the data depends on a single service provider, enterprise will be exposed to the hazard that their data cannot be transferred to different clouds, without the ability of migrating data to additional clouds, users may be required to stay with a cloud if they have significant dependence on the data. Having the whole IT system and data on a single cloud may give the cloud operator excessive power for controlling and modifying users' data. Five deployment models are proposed to handle this security problem and other problems including fault tolerance, service availability, data migration, and data confidentiality and integrity [11].
- Trust: migration to cloud computing environment confers an unprecedented level of trust on to the service provider makes enterprise give up direct control. The customer cannot be sure whether the management of the service is trustworthy or not. Just an authorized document between the customer and service provider called the Service Level Agreement (SLA) can solve this problem, but still there is not clear format for the SLA, and there are services not documented in the SLA that the customer may be unaware that it will require these services at some later time.
- Knowledge of the laws and rules: They vary from state

to another like different rules and laws apply in the European Union versus the United State [6].

- Discuss with the development and engineering team the options that the consumer has in protecting the information that is a part of the cloud migration [5].
- The user have to decide which data, applications and services will remain in the public cloud and which will remain on site behind the firewall or in the private cloud [5].

B. *During data migration*

Migration of data from the existing server to the cloud server is a painstaking task and requires ample skill to handle things, bellow the security requirement in this step.

- Provide Internet Security: The migration process is done via the Internet, so the Internet security must take into consideration when users migrate data from one server to the cloud server.
- Use encrypted file systems. It is the only way to avoid data being snooped while travelling between the enterprise network and the external application is to encrypt it. Even if it is stolen, it will appear as a trash to the third parties, such as the HTTPS protocol for encrypting websites as a third party [5]
- Backups where necessary: Various enterprises are depending on backup when necessary to provide data after the incident. Keep a backup copy at home in the first step to the migration of data from the institution or company to the cloud, as well as the use of alternative cloud and for the same purpose [5].
- Ensure browser updates: Avoid Browser vulnerabilities by deploying in a timely manner [4].

C. *After data migration*

In this step: data has been stored in the cloud, and the main question, how can keep the data in security method and how can access it by security method, away from the snooped.

- Data location: the question here is: how can ascertain whether sufficient commitment are in place, Although the unavailable the location of an organization's data is disclosed to the service

subscriber in many cloud computing services and whether legal and regulatory compliance has been implement strictly enforced. As a solution for this problem, there are external audits and security certifications that can alleviate it. On the other side the destination will the destination continue applying those laws to the data? Will the laws offer additional benefits or risks? [12].

- Authentication and Privileged access: this is known as identity management. Unauthorized access to information resources in the cloud is a significant issue, because of data sensitivity and privacy of information. Therefore before access to applications and data the users need the authentication. There is one solution that can be accomplished in different ways. With the Security Assertion Markup Language (SAML) standard, SAML request and response messages are typically mapped over the Simple Object Access Protocol (SOAP), which relies on XML for its format. For example Amazon Web Services, once a user has established a public key certificate; it is used to sign SOAP requests to the EC2 to interact with it. As well as the authentication of the ability to adapt to user privileges and maintain access to user data; also, there are standards take into consideration as a part of the identity management [12].
- Data segregation: Understanding the use of virtualization by a service provider is a precondition to understanding the risks involved.

TABLE III. CLOUD COMPUTING SECURITY REQUIREMENT

Cloud delivery models	Cloud deployment models	Information security requirement					
		identification and authentication	authorization	confidentiality	integrity	Non- repudiation	availability
Public	IaaS	M	M	O	M	O	M
	SaaS	M	M	M	M	M	O
	PaaS	O	M	O	O	O	M
private	IaaS	M	O	O	O	O	M
	SaaS	M	M	M	M	M	M
	PaaS	O	O	M	M	O	M
hybrid	IaaS	O	O	O	M	O	O
	SaaS	M	M	M	M	O	O
	PaaS	O	O	O	M	O	O
M: Mandatory requirement , O: optional requirement							

- Recovery: In the case of accidents and disasters, can the service vendors' retrieval data, and how is this process enable the seller of the loopback? [13].
- Data availability: Availability is a key decision factor when deciding among (private, public or hybrid) cloud vendors also in the delivery models. By exploring the data security requirements at each of the various delivery models and cloud deployment delivery models set out by the ISO. Enterprises and vendors can be confident in a high protected level in the cloud framework, [13]. We illustrate the cloud security requirements distributed on Cloud delivery models and Cloud deployment models as shown in table III. The requirements are the identification, authentication, authorization, confidentiality, integrity, Non- repudiation, and availability [8].

IV. CONCLUSION

This paper discussed the data migration from an organization's computers to the cloud, including the migration process between clouds as well as workloads migration between different kinds of clouds; Also we have illustrated the security issues: before, during, and after the migration process. The paper focused on security in migration in all the migrations types.

ACKNOWLEDGMENTS

This work was partially supported by the National Natural Science Foundation of China (Grant No. 61173107), the National High Technology Research and Development Program of China (Grant No. 2012AA01A301-01), the Special Project on the Integration of Industry, Education and Research of Guangdong Province, China (Grant No. 2011A091000027) and the Project on the Integration of Industry, Education and Research of Huizhou, Guangdong Province, China (Grant No. 2012C050012012).

REFERENCES

[1] The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology.

[2] Definition cloud migration: http://searchcloudapplications.techtarget.com/definition/cloud-migration

[3] Maintaining Integrity and Security in a Data Migration: http://www.ecommercetimes.com/story/68554.html

[4] Khajeh-Hosseini, A.; Sommerville, I.; Bogaerts, J.; Teregowda, P. Decision Support Tools for Cloud Migration in the Enterprise. In Proceedings of 2011 IEEE 4th International Conference on Cloud Computing, Washinton, DC, USA, 4–9 July 2011

[5] Mr. Shrikant D. Bhopale, Second International Conference on Emerging Trends in Engineering (SICETE), Cloud Migration Benefits and Its Challenges Issue. Dr.J.J.Magdum College of Engineering, Jaysingpur, IOSR Journal of Computer Engineering (IOSR-JCE) ISSN: 2278-0661, ISBN: 2278-8727, PP : 40-45, www.iosrjournals.org

[6] Stephen Kaisler, William H. Money, 2011 IEEE, "Service Migration in a Cloud Architecture".

[7] Definition cloud-to-cloud migration: http://searchservervirtualization.techtarget.com/definition/cloud-to-cloud-migration

[8] Joydipto Banerjee, Kolkata, 2012 IEEE, ''Moving to the Cloud: Workload Migration Techniques and Approaches'',

[9] QingniShen, Lizhe Zhang, Xin Yang, Yahui Yang, Zhonghai Wu, Ying Zhang, 2011 Ninth,'' SecDM: Securing Data Migration Between Cloud Storage Systems''

[10] Cloud data access: Transfer, retrieval no so simple, http://searchcloudstorage.techtarget.com/podcast/Cloud-data-access-Transfer-retrieval-not-so-simple

[11] Gansen Zhao, ChunmingRong, Martin GiljeJaatun, SINTEF, 2010 IEEE, "Deployment Models: Towards Eliminating Security Concerns From Cloud Computing"

[12] Wayne A. Jansen, NIST, Proceedings of the 44th Hawaii International Conference on System Sciences – 2011, '' Cloud Hooks: Security and Privacy Issues in Cloud Computing''

[13] Ramgovind S, Eloff MM, Smith E, School of Computing, University of South Africa, Pretoria, South Africa, sumant.ramgovind@gmail.com; 2010 IEEE, '' The Management of Security in Cloud Computing''.

[14] Xiao Zhang, Hong-tao Du, Jian-quan Chen, Yi Lin, Lei-jieZeng, Department of Computer Science, Northwestern Polytechnical University, Xi'an China, 2011 IEEE, Ensure Data Security in Cloud storage.

[15] Mohit Marwaha, Computer Science And Engineering, Punjab Technical University, Beant College of engineering and Technology, Gurdaspur, Punjab, India. Rajeev Bedi, Computer Science And Engineering, Punjab Technical University, Beant College of engineering and Technology, Gurdaspur, Punjab, India, ''Applying Encryption Algorithm for Data ecurity and Privacy in Cloud Computing''