

# Switching from Vendor Lock-in to the Meta Cloud

B. SandhyaRani<sup>1</sup>, Patil. SivaChandrika<sup>2</sup>

Asst. prof, CSE, RGM College of Engineering and Technology, Nandyal, India<sup>1</sup>

Student, CSE, RGM College of Engineering and Technology, Nandyal, India<sup>2</sup>

**Abstract:** Business locked into cloud doesn't guarantee that the provision of service quality will be continued. By considering the above problem there is a need for the business to permanently caring the cloud that is used and switching to another cloud if problems are discovered. Currently migrating to another cloud is not ignorable. Services like EC2 and S3 are incompatible and doesn't follow specific standards but follow their own. For complicating still more many companies not only build on public on Public Clouds but their own Private Clouds will be combined with public cloud, evolving to the hybrid cloud. The concept of Meta Cloud is introduced that includes runtime and design time components. This Meta Cloud minimizes the technical incompatibilities and thus switching to another cloud. This helps the customers to choose appropriate cloud services for particular appropriate use case.

**Keywords:** Cloud Computing, Meta Cloud, SLA, DSL.

## I. INTRODUCTION

Cloud Computing has been adopted widely in recent years by the organizations. Its major advantage is based on the usage of services on pay-as-per-use basis which is much more convenient. Low cost and scalability make turn towards cloud computing. Even with many advantages many companies are stepping back to look towards cloud because of availability of services and data lock in and legal concerns. Lock in is considered as problem particularly. Even on the high availability of public cloud, a temporary suspension of operation occurs still. The terms and policies of public cloud may change at any time and hence by this the business locked into such a cloud has no middle and longer control on IT costs. The world of computation is becoming large and complex. Cloud computing is emerging as a popular model for computing.

Cloud computing provides several compelling features that make it attractive to business owners that includes, *No up-front investment*: Cloud computing uses a pay-as-you-go pricing model. A service provider does not need to invest in the infrastructure to start gaining benefit from cloud computing. It simply rents resources from the cloud according to its own needs and pay for the usage. *Lowering operating cost*: Resources in a cloud environment can be rapidly allocated and de-allocated on demand. Hence, a service provider no longer needs to provision capacities according to the peak load. This provides huge savings since resources can be released to save on operating costs when service demand is low. *Highly scalable*: Infrastructure providers pool large amount of resources from data centers and make them easily accessible. A service provider can easily expand its service to large scales in order to handle rapid increase in

service demands. *Easy access*: Services hosted in the cloud are generally web-based. Therefore, they are easily accessible through a variety of devices with Internet connections. These devices not only include desktop and laptop computers, but also cell phones and PDAs. *Reducing business risks and maintenance expenses*: By outsourcing the service infrastructure to the clouds, a service provider shifts its business risks (such as hardware failures) to infrastructure providers, who often have better expertise and are better equipped for managing these risks. In addition, a service provider can cut down the hardware maintenance and the staff training costs.

*A. Defining Cloud Computing*: Cloud computing describes a recent trend in information technology (IT) that moves computing and data away from desktop and portable PCs into large data centers that provide on-demand services through the Internet on a "pay as you go" basis. The computing nodes of a Cloud, called *Cloud virtual servers*, are managed by a single administrative domain. Typically, the service offerings of Cloud service providers (*Cloud providers*) comprise access to computing and storage capacity to software platforms for developing and deploying applications and to actual applications.

The main technical underpinnings of Cloud computing infrastructures and services include elasticity, virtualization, service-oriented software Cloud service consumers purchase Cloud services in the form of infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), or software-as-a-service (SaaS) and sell value-added services (e.g., utility services) to end-users. Within the Cloud, the laws of probability give the service provider great leverage through statistical multiplexing of

workloads and easier management, since a single software installation can cover the needs of many users.

Basically clouds can be defined by three types **1)Private Cloud:** Also known as internal clouds, private clouds are designed for exclusive use by a single organization. A private cloud may be built and managed by the organization or by external providers. A private cloud offers the highest degree of control over performance, reliability and security.**2)Public Cloud:** A cloud in which service providers offer their resources as services to the general public. Public clouds offer several key benefits to service providers, including no initial capital investment on infrastructure and shifting of risks to infrastructure providers.**3)Hybrid Cloud:** A hybrid cloud is a combination of public and private cloud models that tries to address the limitations of each approach. In a hybrid cloud, part of the service infrastructure runs in private clouds while the remaining part runs in public clouds. Hybrid clouds offer more flexibility than both public and private clouds. Specifically, they provide tighter control and security over application data compared to public clouds, while still facilitating on-demand service expansion and contraction. On the down side, designing a hybrid cloud requires carefully determining the best split between public and private cloud components.

Traditionally, if the cloud service provider suddenly changes the terms and conditions of the their cloud and if the customers product is in middle of the usage then customer has to proceed his relation with cloud service provider unwillingly and the data of the customer will be locked, in that particular cloud and should pay for cloud usage. To overcome this situation a move to the meta cloud is proposed.

**B. Move towards Meta Cloud:** With the occurrence of lock-in, **Meta Cloud** was introduced to overcome lock-in problem. Most of the recent technologies realize that meta cloud already exists but they are lack of integration. This integration problem in cloud will leads to business lock-in condition. This leads to meta cloud lock-in problem. To avoid meta cloud lock-in, the community must drive the ideas and create a truly open meta cloud. This will add the value for all customers, and will broad support for different providers and implementation technologies. As discussed in above section of *Lowering operating cost*, this feature faces problem in the condition when the CSP's suddenly changes the policies even still the customer's needs CSP's service and at the middle of final outcome.

One of the research challenges of Cloud Computing is Data security, cloud service providers typically do not have accessto the physical security system of data centers, theymust rely on the infrastructure provider to achieve fulldata security. Even for a virtual private cloud, the service provider can only specify the security setting remotely, withoutknowing whether it is fully implemented. The infrastructure

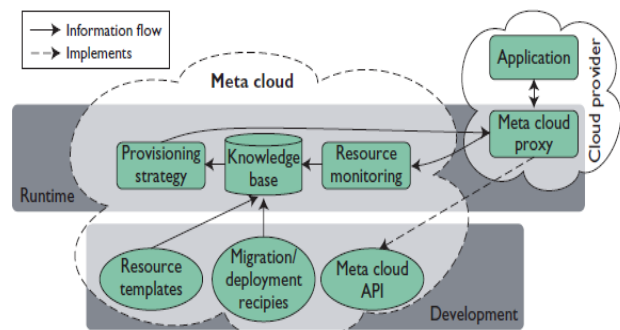
provider, in this context, must achieve the following objectives: (1) *confidentiality*, for secure data access and transfer, and (2) *auditability*, for attesting whether security setting of applications has been tampered or not. Confidentiality is usually achieved using cryptographic protocols, whereas auditability can be achieved using remote attestation techniques. Remote attestation typically requires atrusted platform module (TPM) to generate non-forgeable system summary (i.e. system state encrypted using TPM's private key) as the proof of system security.

## II. IMPLEMENTATION

The problem with the existing system is that once an application has been developed based on one particular provider's cloud services and using its specific API, that application is bound to that provider that is deploying it on another cloud would usually require completely redesigning and rewriting it. Such vendor lock-in leads to strong dependence on the cloud service operator.

With the introduction of the meta cloud concept which incorporates design time and runtime components will be the solution for the problem vendor lock-in. This meta cloud would abstract away from existing offerings' technical incompatibilities, thus mitigating vendor lock-in. It helps users find the right set of cloud services for a particular use case and supports an application's initial deployment and runtime migration. At runtime, an important aspect of the meta cloud is application monitoring, that enables the Meta Cloud to decide whether it's necessary to provision new instances of the application or migrate parts of it. Various vendors provide tools for cloud monitoring, ranging from system-level monitoring (such as CPU and bandwidth) to application-level monitoring to SLA (service level agreement) monitoring. With the meta cloud proposal customers are flexible to choose their best cloud service provider that acts according to their needs.

### A. Inside The Meta Cloud



**Fig 1:** Conceptual meta cloud overview. Developers create cloudapplications using meta cloud development components. [1]

MetaCloud main components are depicted in Figure1. We can categorize these components based on whether they are important mainly for cloud software engineers during development time or whether they perform tasks during runtime

**Meta Cloud API** provides a unified programming interface to theoretical from the differences among provider API implementations. For customers, using this API prevents their application from being changed with new software to a specific cloud service offering since every cloud service provider does not work on same technology and standards, they probably differ.

**Resource Templates** are used to run an application necessary to describe the cloud services by developers. Developers create the meta cloud resource templates using a simple domain-specific language (DSL) (to solve problems in a particular domain and is not intended to be able to solve problems outside it). Using DSL, developers model their application components and their basic runtime requirements, such as CPU, memory, and I/O capacities, as well as dependencies and weighted communication relations between these components.

**Deployment recipes** are an important ingredient for automation in the meta cloud infrastructure. Automation tools such as Opscode Chef provide an extensive set of functionalities that are directly integrated into the meta cloud environment.

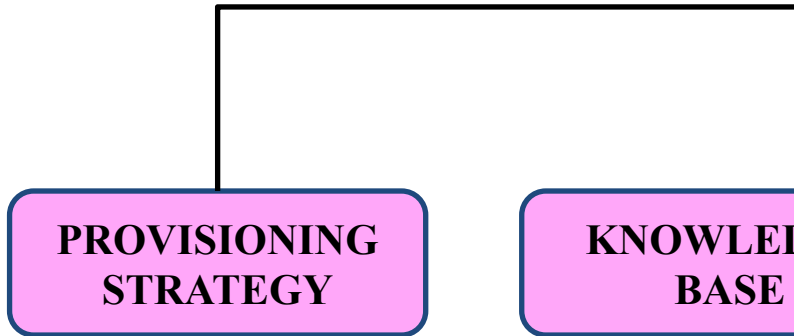
**Migration recipe** describes migrating an application during runtime — for example, migrate storage functionality from one service provider to another. Recipes only describe initial deployment and migration; the **provisioning strategy** and the **meta cloud proxy** execute the actual process using the automation tools.

**Meta Cloud Proxy** serves as mediator between the application and the cloud provider. These proxies expose the meta cloud API to the application, transform application requests into cloud-provider-specific requests, and forward them to the respective cloud services. To avoid high load and computational difficulties, communication between proxies and the meta cloud is kept at a minimum.

**Resource Monitoring** component on an application's request collects data by meta cloud proxies about the resources they are using. The component filters and processes these data and then stores them on the knowledge base for further processing.

**Provisioning strategy** component primarily matches an application's cloud service requirements to actual cloud service providers. It finds and ranks cloud services n based on data in the knowledge base. At runtime, the component can monitor about whether migrating a resource to another resource provider is beneficial based on new insights into the application's behaviour and updated cloud provider QoS or pricing data.

**Knowledge base** stores data about cloud provider services, their pricing and QoS, and information necessary to estimate migration costs. The knowledge base indicates which cloud providers are eligible for a certain customer.



**Fig 2:** Data from Owner to Meta Cloud

for all customers and broad support for different providers and implementation technologies.

#### IV. CONCLUSION

Cloud Computing has wide range of application and has high flexibility towards its usage of services. Cloud service providers incurs with additional cost to the users even they are not satisfied with the vendors specifications with given vendor lock-in. There should be freedom for the user to migrate to another vendor without paying additional cost. For this lock-in problem meta cloud provides the solution and this meta cloud should be implemented as a open cloud.

#### ACKNOWLEDGMENT

We would like to express my heartfelt thanks to (drika) ta of gratitu professt ering and ggestions in journal paper.

#### REFERENCES

1. Benjamin Satzger, Waldemar Hummer, Christian Inzinger, Philipp Leitner, and Schahram Dustdar, "Winds of Change: From Vendor Lock-In to the Meta Cloud," IEEE CS Press, 2013, pp. 69-73.
2. M. Armbrust et al., "A View of Cloud Computing," *Comm. ACM*, vol. 53, no. 4, 2010, pp. 50-58.
3. B.P. Rimal, E. Choi, and I. Lumb, "A Taxonomy and Survey of Cloud Computing Systems," *Proc. Int'l Conf. Networked Computing and Advanced Information Management*, IEEE CS Press, 2009, pp. 44-51.
4. J. Skene, D.D. Lamanna, and W. Emmerich, "Precise Service Level Agreements," *Proc. 26th Int'l Conf. Software Eng. (ICSE 04)*, IEEE CS Press, 2004, pp. 179-188.
5. Q. Zhang, L. Cheng, and R. Boutaba, "Cloud Computing: State-of-the-Art and Research Challenges," *J. Internet Services and Applications*, vol. 1, no. 1, 2010, pp. 7-18.
6. M.D. Dikaiakos, A. Katsifodimos, and G. Pallis, "Minersoft: Software Retrieval in Grid and Cloud Computing Infrastructures," *ACM Trans. Internet Technology*, vol. 12, no. 1, 2012, pp. 2:1-2:34.

#### BIOGRAPHIES



**B. Sandhya Rani** received the B.Tech degree in computer science engineering from the Alfa college of Engineering and Technology, Allagadda, and the M.Tech degree in computer science from the St. Johnes College of Engineering and Technology, Yemmiganur. She is currently working as an Assistant Professor in Department of Computer Science in RGM College of Engineering and Technology, Nandyal.

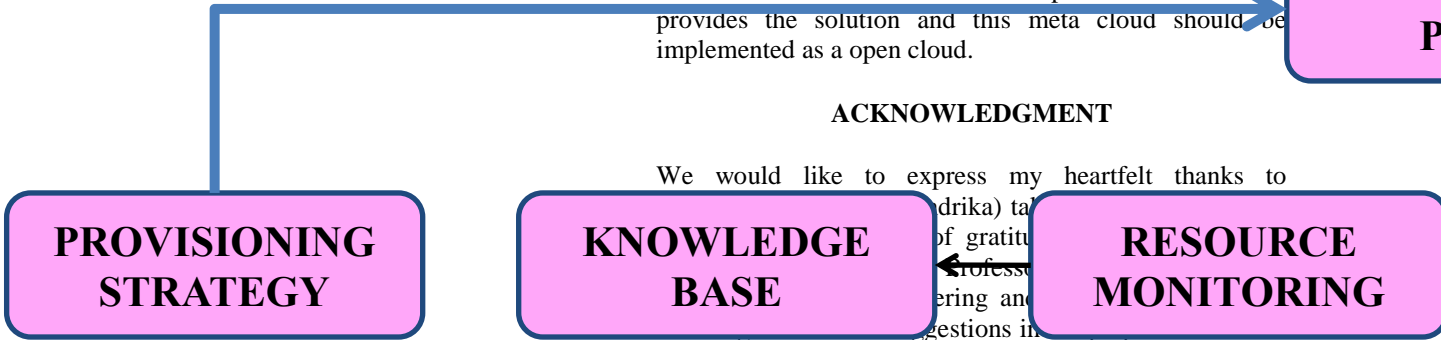


Fig 3: Data from Meta Cloud to End User

In the figures 1 and 2 shows the data flow according to the figure 1 architecture but in view of security, trusted third party (TTP) can be involved in meta cloud and the TTP will not be having any permissions to manipulate the content that is stored in the cloud, it just work on behalf of the two ends. The User of the application can download the file uploaded into cloud by owner of the file, only on TTP verification. If the CSP attempts to modify the content of the file then the application prevents that action and the alert will be immediately sent the owner of the file and the alert includes details regarding the identification of the 'modification attempted CSP. The owner on his choice he can switch to another CSP. For the file security, owner generates random key using which the uploaded file content will be encrypted.

#### III. FUTURE WORK

Most of the basic technologies necessary to realize the meta cloud already exist, but they lack integration. To avoid meta cloud lock-in, the community must drive the ideas and create a truly open meta cloud with added value



**Patil Siva Chandrika** is doing her M.Tech in RGM College of Engineering and Technology, Nandyal and received B.Tech in Information Technology from G.Pullaiah College of Engineering and Technology, Kurnool, She has published two papers in International journals and a

Member of CSI