An Investigation of the Effect of Cloud Computing on Network Management

John Panneerselvam¹, Lu Liu¹, Richard Hill¹, Yongzhao Zhan², Weining Liu³
¹School of Computing and Mathematics, University of Derby, Derbyshire, United Kingdom
²School of Computer Science and Telecommunication Engineering, Jiangsu University, Jiangsu, China
³Key Laboratory of Dependable Service Computing in Cyber Physical Society of the Ministry of Education, Chongqing University, Chongqing, China
l.liu@derby.ac.uk

Abstract- Cloud computing is one of the fascinating advancements in the computing technology. With its fashionable features, cloud deployment is well spread in a wide range of applications. Managing the cloud environment is a complex process because of the virtual nature of the cloud. Cloud management is different from the conventional network management in many aspects. This paper summarizes the functionalities and the importance of network management and reveals the effect of cloud computing over the conventional network management. The five functional areas defined by ISO for network management are mainly concentrated: fault, configuration, accounting, performance and security. Some of the issues faced by cloud computing and their effect in cloud performance have been discussed. Some principles for the network management to support cloud computing and to solve the issues of cloud computing are also suggested. As an important outcome of this academic work, the effects and impacts of cloud computing over network management policies have been delivered to a reasonable depth.

Keywords-cloud computing; network management; virtual computing

I. INTRODUCTION

In the cloud computing technology, cloud providers offer services to the end users through the internet. A cloud can be viewed as a virtual pool of resources that are accessed through the internet. An end-user needs a local machine to get access to the cloud. The interaction between the local machine and the cloud is enabled by the Application Programming Interface (API). Every cloud provider can have their own APIs. Most of the clouds relay on the internet based interfaces which are simpler than the Application Programming Interfaces. Cloud computing could be the right solution for those complicated applications under financial crisis. The contributions of this academic paper are believed to be important as the computing world is gradually transiting to a new era called cloud computing.

Cloud computing provides three types of cloud services such as Software-as-a-service (SaaS), Infrastructure-as-a-service (IaaS), and Platform-as-a-service (PaaS). SaaS enables the users to reach the software that is provided as a service in the cloud without installing the software in their local machines. An example of a SaaS provider is Google Apps. In PaaS, users can use a development kit which is available in the cloud. Microsoft Azure is one of the leading PaaS clouds. IaaS allows the users to execute the cloud software by installing them in their local machine. IaaS mostly targets the hardware components of the local machine and hence it is also known as Hardware-as-a-service (HaaS). Amazon EC2 is an IaaS cloud service.

Public cloud, Private cloud and Hybrid cloud are the three types of clouds in cloud computing. Public cloud is an open pool of resources that can be accessed by all the users. Private clouds are owned by individual organizations. The accessibility of the cloud services [1] is provided only to the particular employees of the corresponding organization in private clouds. Hybrid cloud combines both the public and the private clouds. Hybrid clouds offer services to a well-defined number of users. The service over cloud computing involve five different layers such as client, application, platform, infrastructure and server. A wide range of cloud providers are available in today’s market and according to their service offering capacity, the cloud providers can be classified into local providers, regional providers and global providers.

The important characteristics that make cloud computing fashionable are loose coupling, strong fault tolerance, low-cost, ease use and being service oriented. Loose coupling [2] is a key technical feature that ensures the consistent operation of the cloud though a part of it fails. If an application is interrupted during its runtime, the cloud is tolerant enough to execute the corresponding application by effectively utilising the available resources. Cloud computing is being service oriented and the users seek the cloud only when they need it. The cloud services are dynamic in nature. It ensures that the users need to pay only for the resources accessed by them.

Cloud services are offered at a reduced cost since the capital expenditures are converted into operational expenditures. Elasticity is one of the attracting features of the cloud. The size of the cloud can be expanded or restricted based on the network demand. If the traffic increases during an operation, then the cloud is capable enough to expand its size. Once the network traffic reduces, the cloud automatically restricts its size retaining its earlier allocation.

Cloud computing can be viewed as the advancements of grid computing, parallel computing and distributed computing and it also overcomes the disadvantages found in them.

The rest of the paper is organized as follows. Section II introduces the network management policies of a conventional network. The effect of cloud computing over
The International Organization for standardization (ISO) classifies network management functionalities into five functional areas such as Fault management, Configuration management, Accounting management, Performance management, and Security management. Fault management concerns about the faulty devices and their recovery. Configuration management deals with the initial configuration of the network components and the infrastructure of the network. Accounting management is responsible for the charging and billing functionalities for the utilized resources. Performance management ensures the optimal operation of the network components and security management is responsible for enhancing the network security and distributing the security related information throughout the network. The security policies of the network should be updated consistently for hardening the network against any possible network attacks.

III. NETWORK MANAGEMENT OF A CLOUD ENVIRONMENT

Network management of a cloud environment is different from that of a conventional network environment. Conventional network management involves managing the network devices and the physical links that connect the various network elements together. But, network management of a cloud environment involves managing virtual networks. Cloud management is crucial because frequent errors might lead to the downfall of the entire cloud, if not maintained appropriately. This section illustrates the requirements of network management to support cloud computing in the aspects of the five functional areas of the network management defined by the ISO.

A. Fault Management

In conventional network management, fault management deals with repairing and replacing the faulty devices to retain the network activity. Fault management in cloud computing refers to the ability of the cloud-based virtual network (CVN) to withstand the frequent network changes such as unexpected or extraordinary failures. Strong fault tolerance is one of the key technical characteristics of cloud computing. Fault management plays a vital role in a good cloud environment. Fault management [3] of a CVN depends on two important parameters such as Recovery Point Objective (RPO) and Recovery Time Objective (RTO). RPO is the metric that determines the amount of data to be lost during a disaster. RTO defines the minimum downtime for recovering the faults occurred in the network. A healthy cloud environment should possess a minimum level of downtime and ensures almost zero level of data loss during a fault occurrence.

Using multiple identical network components [4] in a scaled-out fashion will mask the individual failures and thus eliminates the component level failure. These identical network components will stay active all the time in the network. In case of a component failure, one of the active identical components takes over the corresponding operation. Since these identical components stay active during the proper operation of the default network components, this approach is resulting in unwanted usage of the network resources.

An interesting characteristic of virtual networks is their capacity to support automated fault management. If the cloud virtual network fails, the fault management system should be able to restore the contents of the CVN in the internal servers of the cloud provider and transfer the resources to another cloud provider within a reasonable transit time defined by RTO.

B. Configuration Management

A cloud environment involves sharing of multiple cloud virtual networks in a common cloud network infrastructure. Cloud computing can be viewed as an advanced distributed systems and hence stand alone networking is not an ideal solution for configuring the cloud infrastructure. Every CVN consists of more number of Virtual Machines (VMs) and these VMs are likely to be the interfaces of the cloud. Users can get access to the cloud through these virtual machines. Many such CVNs are clustered together to form a bigger cloud. A VM should be able to see the traffic from other VMs that belong to the same CVN in the cloud. The link that interconnects the resources of the cloud is purely logical and the cloud infrastructure should offer a point to point interconnection between the cloud providers and the end users.

Cloud providers assign their own IP addresses to their customers. The clients [5] should make the choice of their cloud and should select the services they required in a process called “on-boarding”. This on-boarding process should be provided with minimum down time by the cloud providers. Cloud deserves a fully automated configuration management system since the manual configuration of
cloud networks is considered to be error-prone. The cloud should be configured as a hierarchical service offering model and based on its hierarchy; it defines two types of users such as end users and median users. End users use the cloud for their own benefit whereas median users act as a bridge between end users and the cloud providers. Cloud users must be able to interact with their own multiple CVNs providers for the purpose of managing their CVN.

CVN Management Interface (CMI) is a well-defined channel that enables the end users to reach the cloud providers. CMI should enable the end users to create, deploy, modify and delete their own CVNs.

C. Accounting Management

Accounting management in both the conventional network and the cloud environment has some common features. The key role of accounting management is to measure the network utilization of both the end and the median users and then to inform the cloud users about their corresponding charges [6] or billing for the resources accessed by them. The accounting functionalities [7] are assigned to Volume Based Billing/Control (VBB/VBC) devices in the cloud infrastructure. In a conventional network, the users will be charged for the resources owned by them irrespective to their utility of the resources. Cloud offers a pay per use service and so the users are charged only for the resources utilized by them. The cloud charging system should be able to start charging instantly after the initiation of the Application Programming Interface (API) and should stop charging once the API is terminated.

Some applications require accessing of multiple resources located in different regions of the cloud. In the elastic application [8] of the cloud, one or more weblets are launched into the cloud in order to expand the cloud resources. Weblets are the micro sites or web pages packed with the user information. In this case, the weblets located in different regions, communicate with each other in order to exchange the data. These weblets are owned by the cloud users and the users lunch their weblets into the cloud to access the resources in the cloud. During the resource usage, the system should be able to charge for the data transfer between the two instances. Charges should be computed as data-out from an instance and data-in to the other instance. If a weblet is involved in data transfer, then it is included in the charging system. The unused weblets are ignored irrespective of their presence in the cloud.

D. Performance Management

Since more number of CVNs are clustered together to form a cloud, it is necessary for cloud service providers to ensure that the individual CVNs are in proper operating condition. This results in a healthy cloud environment as a whole. The performance of each CVN is immune to others in the cloud. Cloud fault recovery system should be designed in such a way that minor faults should be recovered before the cloud actually fails. So, performance management should include consistent monitoring of the cloud status. Each CVN in the cloud should be monitored independently. Monitoring can be achieved through the API. The performance of the applications running on the cloud should also be monitored. Application health monitoring can be employed to monitor the health of the running applications. Network Intrusion Detection System (NIDS) can be employed for passive monitoring for any possible network attacks. Once a fault in detected, the recovery method should be based on whether the fault affects only the particular CVN or it spreads out to the entire cloud.

E. Security Management

Security is one of the major concerns for any network management policies. Security management in a conventional network involves the control of security services and the distribution of security related information throughout the network. In a cloud environment, security management is facing a lot of vital challenges. Since the internet is the communication infrastructure for cloud computing, the security threats of the internet will also play its part in cloud computing. Clouds are vulnerable [7][9] to attacks such as Distributed Denial of Service Attacks (DDoS), IP spoofing, intrusions, worm infections and many.

The most important security role of network management is to ensure a secure usage of the cloud resources from the multi-level cloud providers to cloud users.

Cloud deserves a multi-level security policy that includes authentication, authorization, data encryption, data integration, securing the sessions from hi-jacking and so on. Every client has their own identity for the purpose of authentication. This ensures that the right client is accessing the right resource from the right cloud provider. Confidential data should be subjected to Identity Management to make them harder against the possible network intrusions. Load balancers are suggested by [3] to enhance the network security policies. If not, at least a reverse proxy should be used which makes the cloud infrastructure harder to attack. The firewall in the DMZ should be able to route the traffic towards the right CVN (cloud provider). Every CVN should be configured with their own firewall to regulate the incoming and the outgoing traffic.

IV. NETWORK MANAGEMENT TO SUPPORT CLOUD ISSUES

A. Privacy

Cloud computing requires an architecture that supports privacy to the cloud users at a highest possible level. Separating highly sensitive data [3] from less sensitive data will enhance privacy to the highly sensitive data. Although this work seems to enhance privacy, it gives rise to some critical questions. Which data are to be treated as sensitive? If cloud ensures privacy for the sensitive ones, what about the rest of them?

Privacy is one of the major issues which leads to the downfall of cloud computing. When a cloud user stores his data in the cloud, the data is moved from a single-tenant environment to a multi-tenant environment. Storing the sensitive data in the cloud is different from that of storing them in a local machine. Cloud storage forces the user to
throw his data into the cloud. The user can access the stored data whenever he likes. But, he has no knowledge about the exact location of his data in the cloud and the level of security assigned to his data.

So, this scenario is not encouraging the users to use the cloud memory storage for storing vital information. If the cloud does not assure privacy, users may use the memory options which are in their hands rather than going to the cloud.

To ensure privacy in the cloud, a new conceptual architecture is suggested with some advancement to the work of [3]. Every cloud should be supported by a child cloud. All the data stored by the users in the cloud will be stored in the child cloud. The child cloud is separated from the main cloud by a strong firewall. Also, all the data are encrypted before they enter the child cloud. The cloud users have no direct access to the child cloud. If a cloud user needs to access his data in the child cloud, he sends a request to the main cloud resource. Then the main cloud communicates with the child cloud to access the user information. This ensures a private and permanent storage space in the child cloud for the cloud users. Building up of the child cloud is one of the tasks of the configuration management. The cloud providers are responsible for creating a permanent memory space in the cloud for their hosts. The users are provided with a complete set of knowledge about their storage information and the security features assigned to their data.

The virtual machine in the main cloud and the child cloud should be able to communicate with each other. The VMs should have the capacity to provision instantly for the client requests. This ensures an immediate response of the cloud providers to the client subscriptions even during the failure of the main cloud resource.

A necessary communication link is provided between the virtual machines, so that the information from the main cloud can be updated instantly to the child cloud. The conceptual architecture of the child cloud model is shown in the Fig 1.

B. Cloud Backup

A cloud is a virtual pool of resources. Users use the cloud without any knowledge about the cloud infrastructure. Maintaining and solving the critical issues is the key task of the cloud providers to ensure a good Quality of Service. If the cloud fails, then the entire resources in the cloud will be destructed. So the cloud providers should ensure a powerful backup for the cloud resources. In the event of unexpected overload of the network, the cloud provider should ensure spare [10] cloud services to retain the service being offered to the clients.

The child cloud designed for privacy management can also be used for the purpose of cloud backup. A separate backup of the cloud resources is updated instantly to the child cloud. If the main cloud fails, then the child cloud can be used for recovery.

The child cloud can be used until the cloud resources are transferred to another cloud provider in order to retain the cloud service. It is also necessary for the cloud providers to have a resource backup in their internal resources and this can be utilised if the cloud failure eventually fails the child cloud.

C. Cloud Interoperability

Every Cloud-based Virtual Network (CVN) that forms the entire cloud has its own structure and configuration. So, the cloud users are ending up in a state of chaos in making the choice of their own CVN. This scenario arises when multiple cloud providers club their CVN in a single cloud environment. Every provider has their own way of service offering policies. Network management should ensure a unique configuration and architecture for all the CVNs. This creates uniqueness in the cloud environment and enforces all the cloud providers to offer their service in one common methodology.

As a further development, cloud providers are joining hands to provide collaborated cloud services which involve participation of multiple clouds. Web applications are migrated between the multiple clouds to enable effective cloud service. There is a need for integrating and standardizing the cloud functionalities to enhance the interoperable capacity of the clouds. Secure collaboration “in press” [11] between multiple cloud platforms is very crucial to enable the interoperability functionalities. The major interoperability functionalities of multiple clouds include authentication, authorization, routing, delivery, elasticity and so on. Out of these functionalities, routing is of prime importance as it is likely to be the heart of communication.

The process of routing among multiple clouds involves creation of service instances in the cloud. Every web application has one or more number of service instances [12] in the participating clouds. Routing involves mapping of the corresponding services instances located in different clouds. These service instances can either be created by the clients according to their requirement or by the VMs automatically. Every cloud provider may have their own platform but when integrated, the cloud platform should be able to route the client to the requested cloud. If a cloud
finds the required resources in another cloud, then it uses its own service instance to communicate with the corresponding service instance in the target cloud. The VMs should have the capacity to redirect the applications towards the right client. VM cloning [11] technique can scale well to enhance the redirecting capability of the VMs. The transition [13] of the internet addressing from IPv4 to IPv6 will have a significant effect in the routing mechanisms in the clouds.

User Authentication is one of the key tasks of the service providers during interoperable services. Every cloud provider may have their own way of authentication mechanisms and unique [14] authentication credentials. When users use multiple clouds to perform a single application, authentication is essential with every participating cloud provider. With different authentication credentials, the complexity of identity management increases. Integration the authentication mechanisms to a global standard, will reduce the management complexity provide ease use to the clients.

D. Security Issues

Cloud computing uses the internet as an infrastructure for its communication. Network management should employ all of its internet security policies to cloud computing. An important security consideration highlighted by [3] is the data leakage. When the data is transmitted from the client’s local machine to the cloud, it faces threats during its transmission. The transmission channel should offer the required level of security to the data. Security considerations for addressing such as top-down approach [15] does not scale well for cloud computing. Cloud faces a high rate of security risk in the advent of its interoperability functionalities including routing, migration of the information between multiple clouds, user authentication credentials and many. Using DHT [16] in the open-cloud infrastructure can fortilfy the routing process between multiple clouds. But the non-beneficial complexity [17] of DHT increases the management complexity.

A hierarchical level of security management is required to split up the cloud security tasks into securing the applications, securing the cloud components and securing the host in the cloud.

Securing the application involves an authorization process to block unauthorized accesses and authentication by employing various levels of cryptography. Network Addresses Translations (NAT) and Access Control Lists (ACL) are two important considerations to enhance the security features. ACL should be configured [7] with separate permit and access policies. Securing the network components includes protecting the CVNs and virtual machines in the cloud by ensuring a multi-layer firewall strategy for the cloud infrastructure. Securing the host provides security to the cloud users which in turn allow trusted usage of the cloud resources.

V. CONCLUSION

Undoubtedly, cloud computing is an advance development in the computing technology. Cloud computing is leading the computing world to new insights and innovations. Computing technologies are made much simpler by cloud computing. Now, with the aids of cloud computing, it is possible for a common man to effectively utilise the existing technology without the need of technical knowledge about the technology. But, cloud computing is still in its infant stages and it is facing both technical and management issues. Some of the cloud providers in today’s computing world include Google, Amazon, IBM, and Microsoft. These giant cloud providers together should develop a management standard for effectively managing the cloud environment. Network management should adhere to necessary modifications over conventional management techniques since managing the cloud resources is a different task from that of managing a data centre environment.

This paper summarises the importance of cloud computing in today’s computing world. Some of the key technical and management issues of cloud computing have been highlighted. The areas for improvement over network management to support cloud computing have been discussed. A new concept called child cloud is suggested to enhance the privacy and back up capacity of the cloud. Possible network management solutions for some of the cloud computing issues are also suggested. If these cloud computing issues ends up with the right solution, then it is not very far from now to have a fully efficient cloud environment.

ACKNOWLEDGMENT

The work reported in this paper has been supported by the RLTTF HECloud Programme (Ref: RLTFD005), Visiting Scholar foundation of Key Laboratory of Dependable Service Computing in Cyber Physical Society (CPS-DSC 2012FWJ01), Major Program of the National Natural Science Foundation of China, under contact No. 90818028 and China 973 Fundamental R&D Program (No. 2011CB302600).

REFERENCES


1798


