Trusted Energy-Efficient Cloud-Based Services brokerage Platform

Bandar Aldawsari *, Thar Baker † and David England ‡
School of Computing & Mathematical Sciences, Liverpool John Moores University
Liverpool, United Kingdom
Email: *b.m.aldawsari@2012.ljmu.ac.uk, † t.baker @ljmu.ac.uk, ‡ d.england@ljmu.ac.uk

Abstract

The use of cloud computing can increase service efficiency and service level agreements for cloud users, by linking them to an appropriate cloud service provider, using the cloud services brokerage paradigm. Cloud service brokerage represents a promising new layer which is to be added to the cloud computing network, which manages the use, performance and delivery of cloud services, and negotiates relationships between cloud service providers and cloud service consumers. The work presented in this paper studies the research related to cloud service brokerage systems along with the weaknesses and vulnerabilities associated with each of these systems, with a particular focus on the multi-cloud-based services environment. In addition, the paper will conclude with a proposed multi-cloud framework that overcomes the weaknesses of other listed cloud brokers. The new framework aims to find the appropriate data centre in terms of energy efficiency, QoS and SLA. Moreover, it presents a security model aims to protect the proposed multi-cloud framework and highlights the key features that must be available in multi-cloud-based brokerage systems.

Keywords*- cloud computing, broker, service provider, aggregation, energy efficiency.*

1. Introduction

Cloud computing (CC) has emerged as a new computing paradigm for outsourcing scalable applications and virtual hardware infrastructure (i.e. computing units) that can be provisioned and released with minimal management from so-called cloud data centres. Cloud data centres can be accessed at any time, from anywhere in the world, via users' heterogeneous machines which are connected to the Internet [1]. Therefore, it represents a shift in the geography of computation, where the cloud resources' physical location is not a barrier for users and providers. In other words, users do not need to worry about where their resources/services are based, and/or how they can be accessed and used. On the other hand, providers can offer their services/resources to anyone around the globe. In fact, cloud providers manage, control and monitor cloud data centres to ensure that the required services/resources conform and guarantee the service level agreement (SLA) contract signed with their customers. The primary economic goal is to make these computational services available for users' needs any time, based on a "pay-as-you-go" billing/pricing model.

Pay-per-use was the spark for cloud users to start heavily using, and relying on, these kinds of service, which allowed them to easily and dynamically scale their services/resources up or down, based on the available resources and the scope of their SLA agreement. This rapid growth in cloud services and resources and cloud users has led to a significant increase in the numbers of cloud providers and cloud data centres. Thus, this issue has led to significant increases in network traffic and the associated energy consumed by the growing infrastructure (e.g. extra servers, switches) required to respond quickly and effectively to user requests. Consequently, cloud users are now facing a very challenging and critical task in selecting appropriate cloud offers and resources to fit their requirements. In addition, if the required recourses cannot be provided by one cloud data centre, the provider will not be able to guarantee quality of services (QoS) and SLAs. One approach that could help to solve this situation would be to enable users and their applications to be scaled out across multiple cloud data centres [2].

However, there are three main barriers hindering the implementation and success of the above solution: (i) the lack of computing standards that must be utilised and used by these heterogeneous data centre platforms, which obstructs communication, cooperation and coordination between providers and results in "vendor lock-in" to one data centre; (ii) this has, in turn, made customers totally dependent on using services and resources from one cloud provider, a situation which is known as "customer lock-in", or otherwise leads to substantial switching costs to change provider, which goes against cloud computing ambition; (iii) the increasing number of data centres being used in the multi-cloud requires a significant amount of energy for sending, receiving and processing users' jobs, taking into account that each data centre consumes as much energy as 25,000 households [3].

Therefore, the only practical way to overcome the above issues/barriers is by using an intermediate cloud service broker [4]. According to NIST [5] a cloud broker "is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers". This definition is very broad and overlaps with the cloud service provider role itself.

However, NIST was very specific in identifying the key tasks of the cloud broker to be:

- Service intermediation: improving specific services by creating value-added services to consumers.
- Service aggregation: integrating and combining services into one or more new services.
- Service arbitrage: choosing services from multiple providers.

However, the above three tasks have not been practically developed as yet, nor has much interest been shown in an energy efficient multi-cloud environment. In addition, Wood [6] highlighted the expected cloud brokerage market growth, at a compound annual growth rate (CAGR) of 45% between 2014 and 2018. By taking into consideration the expected growth and the problems shown above, NIST and Gartner [5], [7], respectively, have identified a cloud broker to be the key concern for future cloud computing technology research and development.

An evolving trend in utility and cloud computing patterns, where charges are made to users in accordance with their needs as well as application of security features is called Security-as-a-service (Sec-a-a-S)[8]. Therefore, there can be application of different levels of security as a service every time it is required on a pay-as-you-go ground. Nevertheless, there will be a constant need of Sec-a-a-S application, maybe in every process when system is running, due to access of cloud broker that might need security at various stages and levels that will have specific roles and services. Hence, the calling and injecting of the service in the system will be problematic and expensive. However, this can be easier is the process is finalised during the time of design. Thus, it can be observed that safe cloud service brokerage, that is, role-based access control and differing perceptions on how systems should be configured, observed and applied as well as the requirement to be accomplished to carefully apply the system since flexibility is not observed in many cloud brokerage models methods, is associated with various main interferences [9]. A security-oriented model is thus established in such Multi-Cloud Environment to try and protect cloud service brokerage and properties that have been stored and handled in the cloud and current rational assurances of services' performance and dependability.

The remainder of this paper is organised as follows: section 2 provides a literature review related to brokerage system, energy efficiency and security in the cloud, section 3 discusses the limitations of existing cloud brokers. Section 4 presents the proposed energy-efficient model. Section 5 discusses the network security and the associated issues, and section 6 presents the propped security model. Finally, section 7 highlights the future work that we need to focus on.

2. Literature Review

2.1. Multi-Cloud Broker Architecture

InterCloud [10] is a resource management setting which aims to connect different data centres with each other in order to dynamically coordinate load distribution between various Clouds based on the topology shown in Fig. 1. In this approach, an application can be scaled out between different data centres that are geographically dispersed around the world. Mostly, the resources are close to the users in order to make the process more efficient. However, this study does not consider energy efficiency; as the application scales among different geographically areas, there is a need for an energy conception matrix.

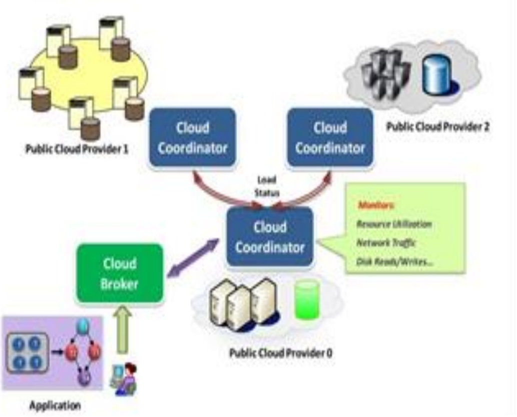

Figure 1. Network Topology of Federated Data Centres [10]

Another broker system has been proposed by Yang et al. [11]; the aim is to solve the problem of transferring bulk data in cloud computing, which lead to problems of reservation and resource utilisation. In this system, the broker's job is to reserve and select combined resources and to assign the best to users. To select the best matched combined resources in a dynamic way the broker defines a new algorithm. Moreover, based on the user's requirement, the broker is responsible for submitting and accepting the request after checking the available data resources and network status. However, scheduling can be the solution here; it can help to allocate the user's requests to available correct resources and can be built into the integration model.

Gatziu et al. [12] have designed a new cloud broker system which can manage and govern the clouds for business modules. The broker here can react to the changes in the business process by scaling the configurations up or down or choosing a new provider. This system performs different roles such as service selection and integration, understanding business processes and analysing and detecting non-explicit changes. However, an interface for such a system is needed to enable consumers to select suitable services. Fig. 2 explains how this broker handles changes.

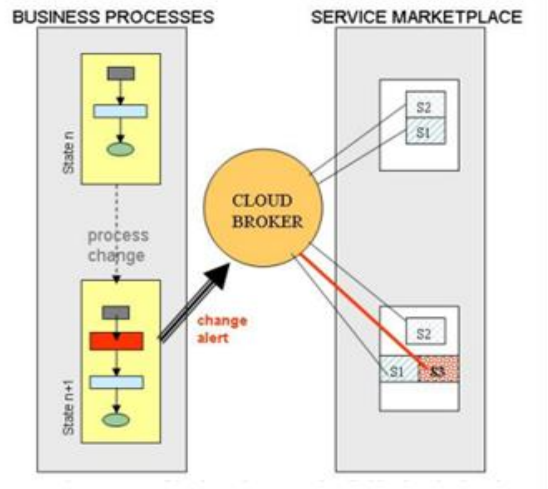

Figure 2. How Changes Are Handled By Cloud Broker [12]

Usha et al. [13] proposed a broker framework architecture that can chose and select the best service providers from amongst many, based on analyses of the QoS requirements. They use Pareto analysis to decide the suitable cloud provider based on two QoS parameters, response time and throughput. In this system, an algorithm has been defined to obtain users QoS requirements along with the parameters that are suitable for them. They concluded that this system aims to select the appropriate cloud service providers with the given criteria to share its resources. The cost of the services should be considered here. Yet, Usha et al. restricted their study to only two QoS parameters: response time and throughput.

Smart cloud broker [14] is a software tool, which allows consumers to choose from different 'infrastructure as a service' (IaaS) clouds and buy the one that meets their business needs and technical requirements. Moreover, it allows consumers to compare the performances of different (IaaS) offerings. In this study, the authors focus on benchmarking as a single way to measure and verify the performance of computing resources. Specifically, they conducted an application stack benchmarking approach to measure the actual performance of the application. This broker can enable service interoperability by developing and using services in multiple clouds through a unified interface. However, in this system there is no consideration for energy efficiency in relation to energy consumed by the datacentre. Moreover, this architecture cannot assure the best match of service provider to user.

Hamze et al. [15] proposed a framework for self-establishing an end-to-end service level agreement between multiple cloud service providers and the cloud user. They focused on QoS for IaaS and 'network as a service' (NaaS) services. This inter-cloud broker works as an intermediate layer between cloud service users (CSU) and cloud service providers (CSP) to help establish the service level required by users to secure the integration process. In addition, they included the network service providers (NSP) in the architecture in order to provide bandwidth on demand. Hence, the CSP's job is to provide both IaaS and NaaS services. However, this study does not show the way in which brokers monitor SLAs at all levels in multiple clouds.

Han et al. [16] developed a cloud service framework for the cloud market using a recommender system (RS) which can help consumers to choose suitable services from multiple cloud providers that match their requirements. To assist users in making decisions, they use network QoS and service rank analysis of resources provided by cloud providers. QoS takes account of execution time, average execution time, response time, average response time etc. While the service-rank considers the quality of virtualization used by many different platforms. However, their framework is limited only to issues related to IaaS. Moreover, the study does not consider energy consumption in a multi-cloud. Fig. 3 shows the architecture of the cloud resource recommendation system.

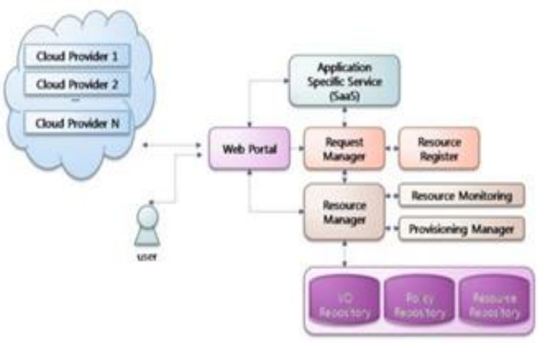

Figure 3. Cloud Resource Recommendation System [16]

2.2. Cloud Energy Efficiency

Gattulli et al. [17] presented a new routing strategy to reduce the cloud network CO2 emissions by dynamically routing/transferring the on-demand energy-intensive data processing requests, via IP-over-WDM networks, to data centres that are powered primarily by renewable energy sources such as wind and solar. However, it can be seen clearly that this solution helps to reduce CO2 emissions at data centre level only.

Other complementary research shown in [18] studied the energy consumption in both the data centre and in data transportation to data centres. Researchers have used optical networks and virtualisation in IP-over-WDM architecture to save power in the data centres and achieve green communication. Two models are proposed in that research:

- Delay-minimized provisioning (DeMiP), which aims to select the nearest data centre based on pre-computed distances between nodes in virtual topology, and then virtual links from the virtual topology are mapped on the physical topology by utilising Dijkstras algorithm for the shortest path.
- Power-minimized provisioning (PoMiP), which focuses on IP routers as power consumers in the transport network and aims to minimise the utilisation of IP router ports. It selects the virtual link with low-power.

An interesting study in [19] presents a cloud energy management system by using a sensor management function and a virtual machine (VM) allocation tool. These sensors are deployed across multiple data centres and can be accessed and monitored via a unified interface for those multiple data centres. The collected data will be used and analysed via the sensor management function through four main phases: monitoring, calculation, analysis and action. The study achieved a 30% energy reduction at data centre level.

In [20] Goudarzi and Pedram found that the cloud providers can reduce total energy consumption by using VMs and server consolidation. This new way of virtualisation can assign tasks through multiple VMs to a single physical server. The study focuses on the VM controller to determine the requirements of the VMs and to be placed on the servers. The framework uses a unique optimisation procedure with the VM controller to minimise energy costs in active servers within the data centre. By enabling consolidation, some of the servers in the data centre will be turned off or put into sleep mode. The study shows that the current servers use only 50% of power in idle mode.

2.3. Trusted Cloud-Based Systems

The platform could sufficiently be made effective by providing cloud computing with the six Trusted Computing elements [21]. This feature of secure computing is still undeveloped ; though, reliable cloud computing services are being designed by various works [22]. The area where the fundamental infrastructure and also the datacentres and interconnection networks are protected is amongst the initial, most natural areas, where the practice of cloud computing is trusted. Evidently, cloud resources could be secured and be separated in virtualised environments if the operational deployment of encrypted data storage, memory curtaining, and secured execution areas, maybe in terms of particular form of the Trusted Platform Module (TPM) architecture contributes significantly [23]. Additionally, shared modules could be protected or limited or incursions be detected when there is application of various methods including watermarking. Furthermore, access to cloud resources could be controlled through with secure end-to-end networking and trust-based reputation systems. Eventually, trusted network zones could be determined by combination of reputation systems with strong Identity and Access Management (IAM), where role-based access control could also be applied.

Table.1 shows a comparison between the multi-cloud broker architectures that are mentioned above.

Table 1. Existing Broker Architectures

Models	**Factors**				
	Energy Efficient Data Centre	Data transporting Energy Efficiency	Quality of Services (QoS)	Service level Agreement (SLA)	Security Model
Federated Inter-cloud[10]	✗	✗	✓	✗	✗
Service-Oriented Broker[11]	✗	✗	✓	✗	✗
Event-Based cloud broker[12]	✗	✗	✓	✓	✗
Efficient QoS cloud broker[13]	✗	✗	✓	✓	✗
Smart Broker[14]	✗	✗	✗	✓	✗
Autonomic Brokerage Service[15]	✗	✗	✗	✗	✗
Recommendation System[16]	✗	✗	✓	✗	✗

3. Limitations of Existing Cloud Brokers

As mentioned above, the broker should act as a bridge between customers and providers in order to enable them to talk to each other and negotiate a certain service(s) using a standard language. The existing, and well known, cloud brokers suffer from the following issues:

- They are implemented as data centre platform dependent systems, and thus they are not sufficient to work with other heterogeneous platforms and infrastructure, which is an essential feature for a multi-cloud service broker.
- There is no standard multi-cloud service broker reference model and architecture that should be utilised by available brokers.
- There is no standard multi-cloud service search and integration engine that could work both horizontally between available data centres in a multi-cloud context, and vertically

between cloud services layers (i.e. IaaS, PaaS and SaaS), to help users to find best-fit services, according to their SLA, and integrate them to serve their needs.

- There is no standard multi-cloud based service/resource modelling and description language that can be exploited by cloud service providers to describe their services and offers to brokers which can also be used by brokers to introduce and offer the available services to their users.
- There is a lack of a quality assurance and service optimisation framework, to evaluate SLAs, detect the failures and protect the system.
- As yet, there is no single cloud broker model to consider the energy consumption in such a multi-cloud environment to minimise the energy that is consumed by cloud parties when sending and receiving data and services.

There is a lack of service management and automation tools that enable customers to create their services portfolio based on legal, financial and operational criteria, which can be scaled up, down and out

4. Proposed Model

4.1. Overview

Our proposed model seeks to solve energy consumption issues in broker systems and provide a high QoS based on the SLA. It will be designed to find the appropriate data centre in terms of energy efficiency and QoS in multi-cloud environments. Therefore, energy efficient routing solutions for cloud computing are required to ensure environmental sustainability. The data centre's energy consumption has prompted a great deal of interest and work in recent years; however, efficiency in cloud computing network energy consumption is still in its infancy and requires further research and development to be fully achieved. There are two main pillars for energy consumed during cloud computing that should be dealt with efficiently and equally to achieve a fully green cloud computing network: (i) the amount of energy consumed at the data centre and (ii) the amount of energy consumed in transporting data between the user and the cloud data centre. The current state-of-the-art solutions focus primarily on improving the energy consumed at the data centres. We propose and evaluate a high-end routing algorithm to fill the gap. It should act as an intermediate bridge for directing the user's requests to green data centres based primarily on using the most energy efficient route to achieve a fully green cloud computing network while making sure the user's requirements, e.g. response time, are met. To accomplish this aim, we model the cloud computing network and its power consumption to compute the energy required by the cloud network before and after using the algorithm proposed in[24] .

We will then formalise the interconnection between the cloud user and a green data centre by using a situation calculus model to define the logical state of the network. Once the interconnection is established and formalised, we then start calculating the time and energy required for both transportation and computation. A linear programming approach will be used thereafter to model the proposed algorithm, which will finally be evaluated against the well-known shortest path routing policy. Fig. 4 shows the proposed cloud broker system.

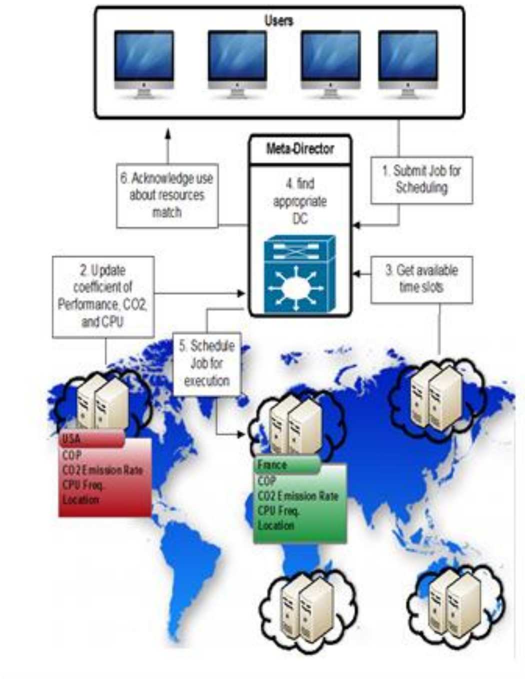
Users
Meta-Director
4. find appropriate DC
6. Acknowledge use about resources match
1. Submit Job for Scheduling
2. Update coefficient of Performance, CO2, and CPU
3. Get available time slots
5. Schedule Job for execution
USA
COP
CO2 Emission Rate
CPU Freq.
Location
France
COP
CO2 Emission Rate
CPU Freq.
Location

Figure 4. Cloud Broker Overview

4.2. Basics and Rules

To achieve green data centres, we use the following assumption throughout our modelling:

There are n green data centres to which a user machine I can be connected through the internet, to accomplish a certain task.

Therefore, one of these available data centres will be used; it must be accessible via the selected most energy efficient route. In other words, amongst multiple routes to a green data centre, the most energy efficient route will be chosen by the new framework.

4.3. Modelling power consumption within the network

Modelling the power consumption of the cloud network is an essential part of this work. One of the most widely accepted methods for modelling power consumption for massively distributed network infrastructure, such as a cloud network, is based on the specifications of telecommunications equipment (i.e. once the quantity and type of equipment in the network are known, the energy consumption of the equipment can easily be calculated). However, this approach alone cannot predict or show the actual network architecture and structure. Once the network architecture is known, then required components can be identified and energy consumption can be calculated accordingly.

A telecommunications network-based model is an essential approach which must be used side-to-side with our model to fill in the gap. In this approach, the network is partitioned into a number of parts: access network, metro/edge network, core network, data centre and IPTV web services network. The network model presented in Fig. 4 is a first-cut of such a massively distributed network and, as such, it does not include many of the fine details of the true network structure and topology. However, it does show the main network architecture and the required components which are needed for the calculation of energy consumption. The energy consumption of the network is calculated using manufacturers' data on equipment quantities and energy consumption, for a range of typical types of equipment, for each part of the network. Using a combination of the above two approaches helps to calculate the power consumption of the entire network using real world network infrastructure components, and it also helps to predict the growth in power consumption dependent on the network architecture and the equipment inventory statistics and their historical sales figures provided [ED2] by the manufacturers.

4.4. Modelling user connectivity to data centre

Using the algorithm proposed in [24], The interconnection between a user machine *i* and a data centre *DC_i*, is based on the public cloud structure shown in Fig. 5 above, which will be formalised as a graph. Thus, between any *i* and a DC_i, we assume that we have an interconnection graph $G^i = (V^i, T^i, P^i, C^i, E^i, L^i, B^i)$ where V^i gives a list of all possible nodes available between any *i* and a *DCi*; and T^i : $V^i \rightarrow \{1,\ldots,6\}$ states the nodes' types, which can be any of six available different types of node, as follows; each node *v*, where $v \in V^i$, might be: an Ethernet switch *(T(v) = 0)*, a broadband gateway router *(T(v) = 1)*, a data centre gateway router *(T(v) = 2)*, a provider edge router *(T(v) = 3)*, a core router *(T(v) = 4)*, and a high capacity Wavelength Division Multiplexed (WDM) transport equipment/links *(T(v) = 5)*, which can interconnect the core routers, as part of the public Internet.

P^i *(v)* and C^i *(v)* states the power consumption and the capacity of a node $v \in V^i$, respectively.

$E^i \subseteq V^i \times V^i$ Defines the interconnection nodes; $L^i : E^i \rightarrow \mathbb{N}$ gives the latency between connected nodes E^I; and finally B^idenotes bandwidth.

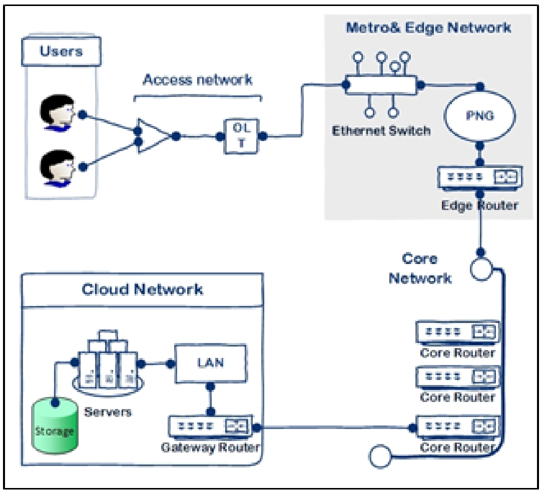

Figure 5. Network structure

4.5. Energy required for transportation

For any user's job to be processed, we assume that we have: the quantity of *Flops* that it requires w_u; the number of input bits in_u to be processed; and the number of output bits ou_u to be returned. Therefore, if we need an energy of ET_{send} *(i)* for sending a bit from the user to the data centre and $ET_{recv}(i)$ for the inverse sending, the total energy transportation cost required for processing J_u is: $in_u.ET_{send}(i) + ou_u.ET_{recv}(i)$. To model $ET_{send}(i)$ *and* $ET_{recv}(i)$, we assume that data sent from a user machine to a data centre is always routed on a path that relies on the two point connection (the shortest path). In using the formulae proposed in [25], the energy required for sending one bit from a user to a data centre is:

$$ET_{send}(i) = 6(\frac{3P_{es}^i}{C_{es}^i} + \frac{P_{bg}^i}{C_{bg}^i} + \frac{P_g^i}{C_g^i} + \frac{2P_{pe}^i}{C_{pe}^i} + \frac{18P_c^i}{C_c^i} + \frac{4P_w^i}{C_w^i}) \quad \textbf{(1)}$$

where in this case, $P_{es}^i, P_{bg}^i, P_g^i, P_{pe}^i, P_c^i$ and P_w^i represent the power consumed by the nodes types listed in subsection 4.4. , Ethernet switches, broadband gateway routers, data centre gateway routers, provider edge routers, core routers, and WDM transport equipment, that are located on the path used for routing a user's job to a *DC$_i$.* $C^i_{es}, C^i_{bg}, C^i_g, C^i_{pe}, C^i_c$ and C^i_w are the capacities of the corresponding equipment in bits per second. The values P^i and C^i depend on the nodes used.

4.6. Time required for transportation

We assume a simple communication model, store and forward, where each node waits for a complete reception of the data before processing it. The approximate time required for sending α bits on a link $e \epsilon E^i$ is equal to max $\{L^i(e),[\frac{\alpha}{B^i_{(e)}}] .L^i(e)\}$.

where, as mentioned in subsection *D* above that, $L^i : E^i \rightarrow \mathbb{N}$ gives the latency between connected nodes $e \epsilon E^i$; and B^i denotes bandwidth. The idea behind this is that either, the bandwidth can contain the bits to send or, we must divide the data to send it in various blocks based on the bandwidth. Finally, we assume that the paths pth_p and $pth_{p'} \epsilon Pth$ were used for sending user data in both directions; then, the total time required for the transportation of a Job J_u in both directions is equal to:

$$Tr(u,i) = \sum_{e\epsilon\, pth_p} \max\left\{L^i(e), \left[\frac{in_u}{B^i_{(e)}}\right]. L^i(e)\right\} + \sum_{e\epsilon pth_{p\prime}} \max\{L^I(e), [\frac{ou_u}{B^i_{(e)}}] . L^i(e)\}$$

(2)

4.7. Energy and time required for computation

We assume that each job J_u will be processed by a single machine in the data centre. We also assume that each data centre DC_i is made of a finite set of homogeneous machines that consume *EP(i)* for processing one flop. Therefore, for processing a job J_u, the data centre DC_i will consume w_u*:EP(i).* Finally, any machine in a data centre DC_i needs approximatively $\mu(i)$ time units for processing one flop. The job J_u can then be processed in approximatively $w_u.\mu(i)$ times units.

Table 2. Energy Efficiency Algorithm

Algorithm1 Input, Output, Steps
INPUT: Jobs J_1, …, J_m with workloads, inputs and outputs data, and intention files; Data centres DC_1, … ,DC_n with energy consumption per flop and frequency; Interconnection graphs G^1, …G^n
OUPUT: Return the best solution on Z
STEPS: 1. Define, for each i , a set of paths C$\boldsymbol{pth_i}$ that can be used for sending and receiving data. 2. For each i, choose a pair of paths (pth_p , $pth_{p'}$) ϵ C$\boldsymbol{pth_i}$ 3. Compute the resulting values of $ET_{Send}(i)$ and $ET_{Recv}(i)$ (equation 1); 4. For any job J_u and data centre DC_i compute *Tr(u; i)* (equation 2) 5. Run *Algorithm1* and obtain *Z*; if it is the best obtained value then it will be kept. 6. If there is possible combination (pth_p , $pth_{p'}$) that has not been explored, go to 2.

5. Network security

Cloud computing is effectively protected based on broadly distributed, publicly accessible systems, recognising the most common cyber security susceptibilities and threats. A service, which can be made by and network with other entities is also shown by every connected systems as they expose their functionalities (complex or atomic). As such, an important aspect of supporting monitoring systems of cloud computing, specifically cloud brokerage systems, is called secure network connectivity, where connection failures must be prevented by making special care of the connection. This is because the mission critical is dependable and constant access to infrastructure resources of the provider. In this context, there is evaluation of existing effective practice in network management filed, where its application can be applied to cloud computing as a platform, the encryption methods to secure the gathered data, and observing IPS services to protect the whole network infrastructure is also included.

5.1. Security approaches

The infrastructure, based on data security, is effectively protected against attack by traditional network security tools. Any production cloud service vitally protects the network and thus, firewalls, DS monitoring as well as other standard management mechanisms should be applied by any public/private provider to offer adequate security level. Furthermore, Unified Threat Management (UTM) systems, which can establish a kind of more subtle attack characteristics and strong networking mechanisms for the purpose of automatic reaction through activating remedial measures, may be applied [26].

The customer benefit from the fundamental strength that is provided by the cloud broker managing a range of services, provided that the broker uses strong security measures, where utilization of the individual services is vital. However, the whole ground of customer services is possibly susceptible if the tools are compromised. Therefore, extra protection of services might be needed by customers to hinder potential threats.

Protection of the data connection, both into the cloud and in the cloud itself is another main aspect of securing network. As such, an effective level of assertion regarding connection security will be provided through encryption. Secure connections, both into the cloud networks and between datacenters is provided by Transport Layer Security (TLS) connections. There might be a need for options including IP Security (IPSec) and Application Layer security protocols including Secure Shell (SSH) because there might be development of implementation-specific vulnerabilities.

5.2. Network Resilience

Making sure that secure connections are both constant and dependable is another aspect that contributes to protection of cloud brokerage platforms. A consistent and reliable connectivity level, just like any other interference to the service can be both expensive and extremely influence the broader system performance, will be needed after the services are moved into the cloud. Thus, this is identified to have two aspects: a) strengthening the current best-effort IP routing mechanisms in the Internet with additional redundancy and b) mitigating malicious denial of service attacks [26].

Since best-effort routing architecture that mostly proves dependable provides no assurance of end-to-end connectivity, the initial aspect is made important by the essential IP. Therefore, technical failures, heavy load on superseding networks, errors in routing, or other issues, may lead to dropping or failing of connections. Evidently, there can be implementation of various methods to enhance network dependability as severe requirements are present in regard to connectivity. For instance, connection risks can be decreased by making sure that the capacity is not surpassed, where this can be attained through QoS mechanisms. Secondly, more paths from the customer to the cloud, based on offer more connection paths, can be guaranteed by the application of route redundancy [26].

Malicious activity, in the second aspect, may threaten connectivity to the cloud and this can be via Denial of Service (DoS) attacks, where this is currently applied by the Anonymous group in reaction to Julian Assange’s arrest [27]. Many recurrent requests are made by DoS attacks to overpower the infrastructures of the provider, where a particular point in the network is their focus. These DoS attacks are distributed to many sources on the Internet and displayed or developed through the usage of legitimate network services, thus making their detection more complicated. Currently, there have been efforts made to develop countermeasures of diagnosing and overwhelming DoS attacks. These efforts are shown in latest attacks on the CloudFlare system.

5.3. Multi-clouds brokerage Threats

The threats that cloud computing encounter are similar to most corporate networks. The increased number of collaborative parties in a multi-clouds environment such as cloud broker leads to an increased number of connections via networked systems and thus increases the system exposure to threats [26]. The major vulnerabilities in cloud computing brokerage system are therefore as a direct result of the ubiquitous nature of using cloud-based networked systems, as follows:

- The system is now able to deliver and integrate services from any location or vendor.
- Authorised users should be able to interact with the services from anywhere at any time.

As a result, there are a number of networking threats that should be considered as relevant here: Insider attacks, Equipment failures, End-to-end issues, Data loss or corruption, DDoS attacks , Cyber threats and hacking attacks, Espionage

These threats may be innocent or malicious; however, the fundamental issue is that the most of Critical Infrastructure is denied access to its data or services or that its confidential data may fall into the hands of another party. Thus, these represent the core requirements that must be met in our work.

6. Proposed security model

6.1. Model Requirements

The security, integrity and exploited service availability will be the three core concerns for brokerage systems. Thus, the major requirements will include: (a) actual time support for such services to offer an effective availability level in the event of faults and recurrent connectivity; (b) scalability to enhance the service to be capable of coping with very bigger volumes of data that are being streamed at a adjustable rate; (c) practical assurance e.g. dependability and flexibility to reduce downtime;(d) legal assurances that can be specified by the customer and then receive a fine extent of control in regard to the service hosting and data repetition strategy applied part of the Service Level Agreement (SLA).

The lack of strong security and user verification in usual cloud platforms as well as the restricted control and observing of replication of data and location of service inside the cloud is the major crucial issues.

6.2. Model Features and Functionality

The fact that functionalities (complex or atomic) as-a-service, which can be made by and involved with other systems that are subscribed to the cloud platform, are exposed by every connected systems makes the main idea of the proposed solutions. The solution given in [26] forms the basis of the suggested solution. The provision of additional data integrity as well as protection to reduce the risk of mission crucial services that are being interrupted or removed by equipment/network failures or attack will be the focus of the model. Thus, about three main services, that is, Service Planning, End-to-End Security, and Monitoring and Policing, as shown in Fig. 6, will be the target.

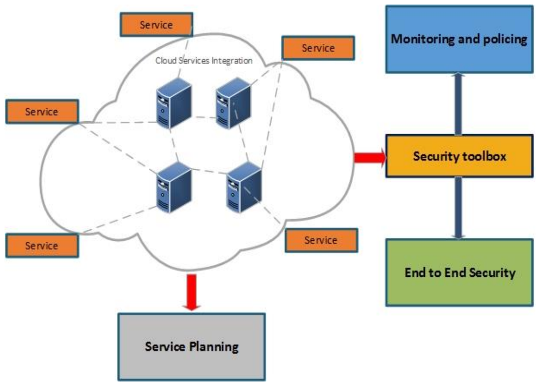

Figure 6. Network Security Model

This model will be then organised as elements in the cloud broker through a ‘toolbox’. However, establishment of a Multilevel User Access Control service, as part in the Monitoring and Policing, will be the focus of this model.

One the other hand, misuse or attack through MultiLevel User Access Control (MLAC) will be protected by the aspect of monitoring and policing with a purpose of making sure that there is security in the system as well as attaining the conditions of the SLA. Establishment of the particular users to gain access to various parts of the platform, in terms of the requirements, will be achieved through replication and extension of broker role-base authentication schemes by the MLAS system. Assurance that the SLA is being applied will be offered to both the user and cloud provider through monitoring. In addition to this, the effectiveness of the platform can be determined by this technique. Furthermore, the cloud will be protected against threats and attacks through offering support to particular UTM systems. Then, strong networking services that are in terms of Software Defined Networking mechanisms will be added to counter the attack patterns are have been identified.

7. Conclusion and future work

This paper presents research related to brokerage systems, energy efficiency and security in the cloud with the weaknesses and drawbacks of current approaches. It highlights the key features that must be available in multi-cloud-based brokerage systems. As yet, most brokers are not sufficiently developed to work with other heterogeneous platforms and infrastructures, which is an essential feature for a multi-cloud service broker. Furthermore, most of the research has yet to consider energy consumption in multi-cloud environments. In order to minimise the energy which is consumed by cloud parties in sending and receiving data, we have proposed a model that seeks to solve energy consumption issues in broker systems, and provides a high QoS based on the SLA. Moreover, we present a security model aims to protect the proposed multi-cloud framework. Future work should focus on designing and developing a novel software- defined broker framework for multi-cloud based service selection and delivery. This necessitates understanding how cloud services are described and how they behave in different data centre platforms and infrastructures to enable brokers to choose and prioritise these services based on users’ needs.

10. References

[1] F. Larumbe and B. Sansò, “Optimal Location of Data Centers and Software Components in Cloud Computing Network Design,” *12th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. (ccgrid 2012)*, pp. 841–844, May 2012.

[2] R. N. Calheiros, A. N. Toosi, C. Vecchiola, and R. Buyya, “A coordinator for scaling elastic applications across multiple clouds,” *Futur. Gener. Comput. Syst.*, vol. 28, no. 8, pp. 1350–1362, Oct. 2012.

[3] J. L. X.-G. L. X.-M. Z. F. Z. B.-N. Li, “Job Scheduling Model for Cloud Computing Based on Multi- Objective Genetic Algorithm,” *Int. J. Comput. Sci. Issues*, vol. Vol. 10, no. 1, p. p134, 2013.

[4] A. Kertesz, G. Kecskemeti, A. Marosi, M. Oriol, X. Franch, and J. Marco, "Integrated Monitoring Approach for Seamless Service Provisioning in Federated Clouds," in *20th Euromicro International Conference on Parallel, Distributed and Network-based Processing*, 2012, pp. 567–574.

[5] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "NIST Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and Technology," *Cloud Comput. Program, Inf. Technol. Lab.*, 2011.

[6] L. Wood, "Research and Markets: Global Cloud Services Brokerage Market 2014-2018: Capgemini S.A., Dell Inc., IBM Corp., Jamcracker Inc. and Liasion Technologies Dominate the Industry," *Reuters, US Edition*, 2014.

[7] Gartner, "Cloud Computing," 2014. [Online]. Available: http://www.gartner.com/technology/topics/cloud-computing.jsp. [Accessed: 20-Nov-2015].

[8] M. M. Hasan and H. T. Mouftah, "Cloud-based security services for the smart grid," *Proc. 2013 Conf. Cent. Adv. Stud. Collab. Res. (CASCON '13)*, pp. 388–391, Nov. 2013.

[9] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology," *NIST Spec. Publ.*, no. 800–82, pp. 1–157, 2011.

[10] R. Buyya, R. Ranjan, and R. N. Calheiros, "InterCloud: utility-oriented federation of cloud computing environments for scaling of application services," *10th Int. Conf. Algorithms Archit. Parallel Process.*, vol. 6081, pp. 13–31, May 2010.

[11] Y. Yang, Y. Zhou, L. Liang, D. He, and Z. Sun, "A Sevice-Oriented Broker for Bulk Data Transfer in Cloud Computing," *2010 Ninth Int. Conf. Grid Cloud Comput.*, pp. 264–269, Nov. 2010.

[12] S. Gatziu, T. Kumar, and W. Holger, "Cloud Broker: Bringing Intelligence into the Cloud An Event-Based Approach," *... IEEE Intl. Conf. Cloud Comput. Miami, Florida*, pp. 6–7, 2010.

[13] M. Usha, J. Akilandeswari, and A. S. S. Fiaz, "An Efficient QoS Framework for Cloud Brokerage Services," in *International Symposium on Cloud and Services Computing*, 2012, pp. 76–79.

[14] M. Baruwal Chhetri, S. Chichin, Q. Bao Vo, and R. Kowalczyk, "Smart Cloud Broker: Finding your home in the clouds," *IEEE/ACM Int. Conf. Autom. Softw. Eng.*, pp. 698–701, Nov. 2013.

[15] M. Hamze, N. Mbarek, and O. Togni, "Autonomic Brokerage Service for an End-to-End Cloud Networking Service Level Agreement," *2014 IEEE 3rd Symp. Netw. Cloud Comput. Appl. (ncca 2014)*, pp. 54–61, Feb. 2014.

[16] S.-M. Han, M. M. Hassan, C.-W. Yoon, and E.-N. Huh, "Efficient service recommendation system for cloud computing market," in *Proceedings of the 2nd International Conference on Interaction Sciences Information Technology, Culture and Human - ICIS '09*, 2009, pp. 839–845.

[17] M. Gattulli, M. Tornatore, R. Fiandra, and A. Pattavina, "Low-carbon routing algorithms for cloud computing services in IP-over-WDM networks," *EEE Int. Conf. Commun.*, pp. 2999–3003, Jun. 2012.

[18] B. Kantarci and H. T. Mouftah, "Optimal Reconfiguration of the Cloud Network for Maximum Energy Savings," in *th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012)*, 2012, pp. 835–840.

[19] F. Satoh, H. Yanagisawa, H. Takahashi, and T. Kushida, "Total Energy Management System for Cloud Computing," in *IEEE International Conference on Cloud Engineering (IC2E)*, 2013, pp. 233–240.

[20] H. Goudarzi and M. Pedram, "Energy-Efficient Virtual Machine Replication and Placement in a Cloud Computing System," in *IEEE Fifth International Conference on Cloud Computing*, 2012, pp. 750–757.

[21] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," *Proc. 2009 Conf. Hot Top. cloud Comput.*, p. 3, Jun. 2009.

[22] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1113–1122, Jul. 2011.

[23] P. Gourbesville, J. Batica, J. Y. Tigli, S. Lavirotte, G. Rey, and D. K. Raju, "Flood warning systems and ubiquitous computing," *La Houille Blanche*, no. 6, pp. 11–16, 2013.

[24] T. Baker, Y. Ngoko, R. Tolosana-Calasanz, O. F. Rana, and M. Randles, "Energy Efficient Cloud Computing Environment via Autonomic Meta-director Framework," in *6th International Conference on Developments in eSystems Engineering*, 2013, pp. 198–203.

[25] J. Baliga, R. W. A. Ayre, K. Hinton, and R. S. Tucker, "Green Cloud Computing: Balancing Energy in Processing, Storage, and Transport," *Proc. IEEE*, vol. 99, no. 1, pp. 149–167, Jan. 2011.

[26] T. Baker, M. Mackay, A. Shaheed, and B. Aldawsari, "Security-Oriented Cloud Platform for SOA-Based SCADA," in *2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 2015, pp. 961–970.

[27] A. Pras, A. Sperotto, G. C. M. Moura, I. Drago, R. Barbosa, R. Sadre, R. Schmidt, and R. Hofstede, "Attacks by ' Anonymous ' WikiLeaks Proponents not Anonymous," pp. 1–10, 2010.