Cloud Computing: Security Issues and Energy Usage

Nazneen Taj¹ & Dr. Anirban Basu²

Abstract: The basic idea of cloud computing is reusability of resources and is built upon distributed computing, virtualization, networking web and software services and utility computing. In cloud computing as we keep the information in our hard drive we save it in internet at an alternate area. All the resources which cost us more when we use it individually will be much less and abundantly available in the cloud network, thus making our requirements satisfied with less investment. Cloud providers generally schedule tasks with redundancy to provide high reliability. Resource and time redundancy correspond to the active replication and backup/restart scheme respectively. For the active replica-maximization scheme, several processors are scheduled simultaneously, and the task will succeed if at least one processor does not encounter a failure. In backup/restart scheme the task will be scheduled on the backup processor when a processor encounters a failure. This paper discusses few of the failure problems in cloud computing and the recent methods used to avoid the failures and make the cloud reliable.

Keywords: Dynamic voltage frequency scaling (DVFS), Virtual Machines (VM), Service level agreements (SLAs), Software as a service (Saas).

1. Introduction:

In cloud computing, large scale clusters, and Grids infrastructure are unified computing platform which tries to connect and share all resources in the Internet, including computation resource, storage resource, information resource, knowledge resource and equipments for scientific research, and then solves the problems of large-scale scientific engineering computing. As the basic feature of cloud are dynamic, heterogeneity, distribution, openness, voluntariness, uncertainty and deception obtaining trust worthy computing resource becomes difficult in large-scale parallel distributed system. For a data-intensive Web server application that publishes significant amounts of data stored in a back-end database should respond to the queries immediately. Thus the performance of these read-intensive applications largely depends on the performance of underlying parallel disk storage systems. Thus reducing the mean response time of parallel disk storage systems is a must for these applications. Instant computing environments provide elevated resource access for time-critical applications and workflows. Severe weather forecasting systems, are time-critical applications these are often deadline-driven and the performance of these workflows is influenced by several Quality of Service (QoS) metrics. with fast development of scientific research, users may make complicated demands like users may try to minimize their payments when guaranteeing their service level such that their tasks can be finished before deadlines. These kind of demands create inevitable errors in predicting task workloads will definitely create the problem of scheduling the resources.

In real time applications it is quiet difficult to ask the cloud users to specify their security demands in detail. While computing power under deadline and budget limits, the cloud customers also express an SD level from high to low. Thus the scheduling of jobs has to take the risk factor into account. In real time a Grid job scheduler must be security-driven and resilient in response to all risky conditions. The scheduler must take into account the risks involved in dispatching jobs to remote sites. Therefore risk-resistant strategies are needed to properly manage the risks it may take[1]. The following fig. 1.1 shows the grid job scheduling.
Cloud computing due to its architectural design and characteristics imposes a number of security benefits, which include centralization of security, data and process segmentation, redundancy and high availability. At the same time risks are countered dominantly, due to the infrastructures singular characteristics, a number of distinctive security challenges are introduced. Cloud computing has special attributes that require risk assessment in areas such as availability and reliability issues, data integrity, recovery, and privacy and auditing. Therefore security is related to the important aspects of confidentiality, integrity and availability which inturn are the building blocks to be used in designing secure systems. These important aspects of security, apply to the three broad categories of assets which are necessary to be secured, data, software and hardware resources[2]. As cloud manages multiple applications in a data center creates the challenge of on-demand resource provisioning and allocation in response to time-varying workloads. Usually, data center resources are statically allocated to applications, based on peak load characteristics, in order to maintain isolation and provide performance guarantees and bit of security[3]. As high performance was what the users and providers were concerned about now much attention is given to security and energy consumption. Thus this paper discusses some concepts about security and the future aspects like energy management that need to be concerned more in the cloud computing environment.

2. Related work:

High security is one of the major issue for making cloud computing as a utility computing. Due to sensitive applications and data are moved into the cloud data centers, run on virtual computing resources in the form of virtual machine poses many novel tangible and intangible security challenges like accessibility vulnerabilities, virtualization vulnerabilities, and web application vulnerabilities. By relating challenges to cloud server having physical control of data, relate to identity and credential management, relate to data verification, tempering, integrity, confidentiality, data loss and theft. To protect private and sensitive data that are processed in data centers, the cloud user needs to verify (a) the real exists of the cloud computing environment in the world (b) the security of information in the cloud and (c) the trustworthiness of the systems in cloud computing environment[4]. These tasks are not so easy and thus the total security of the cloud is a big challenge to the service providers. Therefore to begin with the concept of security, cloud has to be tested. The definition of testing can be given as "cloud testing is a form of software testing in which Web applications that leverage Cloud computing environments ("cloud") seek to simulate real-world user traffic as a means of load testing and stress testing web sites. The ability and costs to simulate Web traffic for software testing purposes has been an inhibitor to overall Web reliability." The testing of cloud has the four major aspects:

1. Assure the quality of cloud-based applications deployed in a cloud, including their functional services, business processes, and system
performance as well as scalability based on a set of application-based system requirements in a cloud.

2. Validate software as a service (SaaS) in a cloud environment, including software performance, scalability, security and measurement based on certain economic scales and pre-defined SLAs.

3. Check the provided automatic cloud-based functional services, like auto-provisioned functions to test cloud compatibility and inter-operation capability between SaaS and applications in a cloud infrastructure and checking the APIs of SaaS and their cloud connectivity to others[5].

Few research paper suggest multitenancy refers to the cloud characteristic of resource sharing. Several aspects of the IS are shared including, memory, programs, networks and data. In cloud computing a business model is created in which resources are shared at the network level, host level, and application level. Even though users are isolated at a virtual level, hardware is not separated. With a multitenant architecture, a software application is designed to virtually partition its data and configuration so that each client organization works with a customized virtual application instance. Multitenancy, is relative to multitasking in operating systems. In computing, multitasking is a method by which multiple tasks, also known as processes, share common processing resources such as a CPU[6]. Thus making the security issue more complicated as the basic structure of cloud is somewhat being in the same home all family members have to hide their confidential secrets from each other to certain level. The threats in cloud computing can be categorised as 1. Multitenancy issues 2. Account control 3. Malicious insiders 4. Data control 5. Management console security. Fig 2.1 shows the pictorial representation of the same.

Researchers[6] also propose that due to the cloud environments unique characteristics, communications are required to be protected not only between users and hosts but also from host-to-host. Choosing IPSec or SSL depends on the diverse needs and security requirements. IPSec is compatible with any application but requires an IPSec client to be installed on each remote device (PC, PDA, etc.) to add the encryption. SSL is built into every browser, so no special client software is required. As the cloud environment promotes use by heterogeneous platforms it is unacceptable to require users to install an IPSec client for encryption. And also as cloud services are mostly accessed through browsers, SSL has many benefits for client to host communications. On the other hand, IPSec supports using compression making it a more efficient choice for host-to-host communications. Researches[6] proposed that by implementing IPSec for encrypting communications for host-to-host communications and SSL for Client-to-Cloud communications security can be better. Fig.2.2 represents the security betterment through self authentication.
When we are using cloud for sharing numerous resources and for the storage not only the security will become a issue even the energy consumed by the data center will also play a dominant role in cloud management. Thus we need to give importance to Green Cloud computing which is envisioned to achieve efficient processing and utilization of computing infrastructure and to minimize energy consumption. This is required for ensuring that the future growth of Cloud computing is sustainable. Cloud computing with increasingly pervasive front-end client devices interacting with back-end data centers will cause an enormous energy consumption. To address this problem, data center resources need to be managed in an energy-efficient manner to drive Green Cloud computing. Therefore Cloud resources need to be allocated not only to satisfy QoS requirements specified by users via Service Level Agreements (SLA), but also to reduce energy usage[7].

Cloud providers have to make ensure that they provide flexibility in their service delivery to meet various consumer requirements for their services, by keeping the consumers isolated from the underlying infrastructure. To support Green Cloud computing, providers also need to minimise the energy consumption of Cloud infrastructure, while enforcing service delivery.

3. Proposed method:

This paper combines certain methods and techniques to solve the security and energy issues in the cloud environment.

Virtualisation technologies provide the ability to transfer VMs between physical nodes using live or offline migration which enables the technique of dynamic consolidation of VMs to a minimal number of nodes according to current resource requirements. Based on the related work that has been discussed in this paper, cloud environment should consider the energy saving as much as possible as possible by using the simple techniques like the idle nodes can be switched off or put to a power saving mode (sleep, hibernate) to reduce total energy consumption by the data center. Despite the energy savings, aggressive consolidation of VMs may lead to a performance degradation and may result in SLA violation. A virtual machine cannot accurately record the timing behaviour of a physical machine which leads to the timekeeping problems resulting in inaccurate time measurements within the virtual machine, which can lead to incorrect enforcement of SLA. All these issues require effective consolidation policies that can minimise energy consumption without compromising the used-specified QoS requirements. Thus by dynamically migrating VMs across physical machines, workloads can be consolidated and unused resources can be put on a
low-power state, turned off or configured to operate at low-performance levels (using DVFS) in order to save energy[7].

To save energy in the cloud data center one should also know the actual energy that a data center is needed both in full load and average load conditions. The energy consumed by the datacenter can be calculated as

\[ E = \int P(u(t)) \text{ d}t. \] [7]

Where E is the energy consumed by the data center, P is the power required by the data center, u(t) is energy utilization with respect to the time.

But where ever the concept of power and energy arises the loses has to be considered because each of the electrical and electronics components we use in the cloud will consume certain amount of energy in the name of voltage drop across it. Therefore we need to modify the above equation and propose a equation by considering the losses.

\[ E = \int P(u(t)) \times L \text{ d}t. \]

The losses are the some of the heat dissipated in the datacenter called heat losses, redundancy losses in the components, losses to due heating of cooler motors etc. Once the actual amount of energy consumed by the data center is revealed we use some energy saving algorithms to reduce the energy consumption. Energy saving can be done in the various forms of scheduling algorithms like DVFS, using the concept of VMs, using sleep modes etc. The objective is to find a trade-off between reducing the energy consumption and preserving the performance of resource nodes. A traditional data center has many distinguished features including heterogeneous hardware, heterogeneous workload, focus on average load rate, and consumption of time and human effort for administrative tasks[8][9][10].

Researchers[1] have proposed heuristics and genetic algorithms which can be used with the energy saving model[8] to save an appreciable amount of energy. Fig 3.1 shows the different scheduling strategies and the algorithms.

<table>
<thead>
<tr>
<th>Scheduling Strategy</th>
<th>Heuristic Algorithms</th>
<th>Genetic Algorithms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risky job execution</td>
<td>Risky-Heuristic: Jobs are scheduled based on a heuristic algorithm without considering the risk factor.</td>
<td>Risky-STGA: Jobs are scheduled based on space-time genetic algorithm without considering the risk factor.</td>
</tr>
<tr>
<td>Preemptive insecure jobs</td>
<td>P-Heuristic: Preemptive job execution due to insecure conditions. Resubmit failed jobs to other sites.</td>
<td>P-STGA: Job is scheduled based on STGA that allows preemption. Resubmit failed jobs to other sites.</td>
</tr>
<tr>
<td>Replicated job execution</td>
<td>R-Heuristic: Replicates jobs to multiple sites to prevent from possible failures (fixed number of replicas).</td>
<td>R-STGA: STGA that replicates jobs to multiple sites to prevent from possible failures (variable number of replicas).</td>
</tr>
<tr>
<td>Delay-Tolerant scheduling</td>
<td>DT-Heuristic: Allows jobs to be delayed for some time when condition is not met before rescheduling.</td>
<td>DT-STGA: STGA that allows job to be delayed for some time, when condition is not met before rescheduling.</td>
</tr>
</tbody>
</table>

Fig. 3.1: Different scheduling strategies and the algorithms used.

Next comes the security issue which involves in various stages of cloud usage by the consumers. The privacy issues differ according to different cloud scenario, and can be divided into four sub-categories, which include: (a) how to make users remain control over their data when it is stored and processed in cloud, and avoid theft, nefarious use and unauthorized resale, (b) how to guarantee data replications in a jurisdiction and consistent state, where replicating user data to multiple suitable locations is an usually choice, and avoid data loss, leakage and unauthorized modification or fabrication, (c) which party is responsible for ensuring legal requirements for personal information, and (d) what extent cloud sub-contractors involved in processing can be properly identified, checked and ascertained[9]. To protect clouds, traditional hard security techniques such as encryption and authorization provide a solid foundation, but they fail when cooperating entities act maliciously due to scale and temporary nature of collaborations. Trust as a soft social security philosophy can fight against such security threats by restricting malicious entities from participating in interactions and consequently offers a high trustworthiness cloud computing environment. Thus this paper propose that by using security at layer level and by the proper authentication of each cloud user we can secure the transactions in cloud[10]. And by calculating the actual amount of energy consumed in the data center we can use appropriate methods to reduce energy consumption in a data center.
4. Conclusion and future work:

The main objective of this paper is to discuss about the security issues in the cloud environment and the energy saving in the cloud data center. This paper briefs some of the security methods which can combine with certain scheduling algorithms to save energy and make the cloud secure to some extent. The related future work of this paper can be implementation of some hybrid algorithms that can save good amount of energy in cloud data center by scheduling the resources and the jobs by using some optimization techniques without lowering the cloud performance.

5. Bibliography


