Available online at www.elixirpublishers.com (Elixir International Journal)

Information Technology

Elixir Inform. Tech. 71 (2014) 24594-24602

ISSN: 2229-712X

Different Aspects in Cloud Computing: A Comprehensive Review

Pabak Indu[1], Souvik Bhattacharyya[1] and Gautam Sanyal[2]

[1]Department of Computer Science and Engineering, University Institute of Technology The University of Burdwan, Burdwan, India.

[2]Department of Computer Science and Engineering, National Institute of Technology, Durgapur, India.

ARTICLE INFO

Article history:

Received: 16 April 2014;

Received in revised form:

20 May 2014;

Accepted: 31 May 2014;

Keywords

Cloud Computing,
Cloud Service Provider (CSP),
Cloud Service User (CSU),
Security Requirements,
Security factors,
Scheduling algorithm,
Third Party Auditor (TPA).

ABSTRACT

Cloud computing can be observed as the transition of a long held dream called "Computing as utility", into reality. This is a next generation platform that provides dynamic resources pods, virtualization, and high availability. The success of cloud lies in the terms "pay per use" and "multi tenancy". But these two major advantages bring some disadvantage with them. The "pay per use" facility requires proper scheduling of tasks for proper utilization of the cloud. And the "multi tenancy" brings some major security threats as all the different organizations use the same physical infrastructure. Many researchers have concentrated in both the fields. In this paper authors have studied various security solutions, scheduling algorithms and their issues related to cloud computing.

Introduction

Cloud computing is a very popular but still evolving field. It allows many organizations to start at a minimum infrastructure cost .NIST(National Institute of Standards and Technology) defines cloud computing as [1] "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". Key features of cloud computing involves "pay-per-use", "multi tenancy", "on-demand-self service", "scalability", "resource pooling".

The cloud has been broadly categorized into four deployment model [2] and three service models [2] as shown in Fig 1.

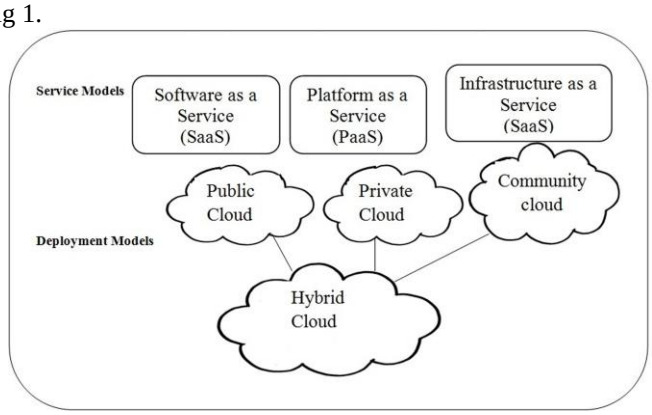

Fig1: Different types of Cloud Service and Deployment Models

The Cloud Service Models:

Software as a Service (SaaS): This model [2] offers a complete application to the client as an on demand service . A single instance of the service runs on the cloud and multiple end users can access that service. On the other hand clients do not need any investment in servers or software licenses but for provider's, the costs are minimized, since only a single application needs to be hosted and maintained. The SaaS Provider's manages the software on "usage" basis. This includes future versions releases, maintenance and patches services etc. Examples of the SaaS [3] model are described below.

Google Apps:

This is a web-based office tools such as e-mail, calendar and document management tools

Salesforce.com:

This cloud provides full customer relationship management (CRM) application.

Zoho:

This cloud provides large suite of web-based applications, mostly for enterprise use.

Platform as a Service (PaaS): This model [2] provides a higher level of development environment form which other higher levels of service can be built. Every client has the freedom to build his own applications which runs on the provider's infrastructure. Examples of PaaS [3] providers are described below.

Akamai Edge Platform:

Large distributed computing platform for web application deployment (focus on analysis and monitoring of resources)

Force.com:

Platform to build and run applications and components bought from AppExchange or custom applications.

Google App Engine:

This is a platform to develop and run applications on Google's infrastructure.

Microsoft Azure Services Platform:

This platform provides on-demand compute and storage services as well as a development platform based on Windows Azure.

Tele:
E-mail addresses: pabakindu@yahoo.co.in, souvik.bha@gmail.com

Yahoo! Open Strategy (Y!OS):

This is a platform to develop and web applications on top of the existing Yahoo! Platform (focus on social applications).

Infrastructure as a Service (IaaS): This model [2] provides basic storage and computational support to the clients over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. Examples of IaaS [3] Providers are discussed bellow.

Amazon Elastic Compute Cloud (EC2):

This service provider provides users a special virtual machine (AMI) [3] that can be deployed and run on the EC2 infrastructure deployed.

Amazon Simple Storage Solution (S3):

This service provider provides users access to dynamically scalable storage resources.

IBM Computing on Demand (CoD):

This service provider provides users' access to highly configurable servers plus value-added services such as data storage.

The Deployment Model

The Deployment Model [2] sets the standards for how and where client's data and applications reside and how they are interacted and protected.

Public Cloud: This Cloud infrastructure [2] is made available to the Cloud Service Users (CSU) and is owned by CSPs like examples are Amazon, Google and Microsoft Azure. In this model CSU refers general public or a large industry.

Private Cloud: This Cloud infrastructure [2] is used entirely by an organization. It may be managed by that company or a third party and it may exist on or off premise. Like Attenda RTI.

Community Cloud: This Cloud [2] infrastructure is shared by several CSUs (like organization, supports a specific community) that has similar interests. Like G-Cloud which of UK.

Hybrid Cloud: This Cloud model [2] is a composition of two or more previous models, which has some unique properties but are bound together by standard rules that remain unique entities but are bound together by some standardized technologies that permits some data and application portability. This is the most popular delivery model.

Characteristics of Cloud:

Lets concentrate on the key characteristics of cloud [4] which makes it more appealing to the present world IT business scenario.

i. *Flexibility of cloud* evolves with user's ability of adapting new technological infrastructure resources.

ii. Cloud environment uses an *application programming interface (API)* which is similar to the traditional interfaces of different types of software. In cloud environment Representational State Transfer (REST)-based APIs are used.

iii. *Cost* is one of the key features of cloud computing. A public-cloud delivery model reduces capital expenditure to operational expenditure [5]. The e-FISCAL project's state-of-the-art repository [6] contains article supporting cost aspect in more details and most of them concluded that the cost of savings is proportional to the type of activities and infrastructure supported by the cloud service provider.

iv. *Device and location independence:* This feature [7] felicitate user to access the system using web browser regardless of their location and infrastructure.

v. *Virtualization* allows sharing of resources and increased utilization. Applications can easily be migrated from one physical environment to another.

vi. *Multi tenancy*. This feature makes the cloud environment more attractive. This feature enables sharing resources and cost among all the users. Which results

a. Maintenance of infrastructure in a single location with lower costs.

b. User does not to worry about load capacity of their infrastructure.

c. Resource utilization increases.

vii. *Reliability* is maintained by the use of multiple redundant sites. This mechanism helps the cloud environment to maintain its services and appropriate for disaster recovery [8].

viii. *Security* maintenance is improved due to storing the entire data under a single site. But main concern about this facility is losing control over certain sensitive data. In spite of the security concern it's much more secure than traditional methods of security.

The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics" [9]:

i. *On-demand self-service.* A consumer can access cloud computing capabilities, such as server time and network storage, as needed, without any interaction to the cloud service providers.

ii. *Broad network access.* Cloud supports different heterogeneous kind of mechanisms or devices to access the environment.

iii. *Resource poling.* A cloud service provider serves many clients and these physical and virtual resources are provided according to their need. The customers are unaware of the fact where the resources are located.

iv. *Rapid elasticity.* Capabilities can be rapidly and elastically changed, i.e. capacity of a cloud can be easily be changed according to the need. In other words it's the scalability factor of the cloud.

v. *Measured services.* As this is a kind of tenancy mechanism so for the business purpose the services are monitored controlled. These information is also used for optimization and controlling the resources.

Table 1(a), Table 1(b) and Table 1(c) draws a comprehensive review on the field of benefits, drawbacks and information security aspect of different cloud service models.

Table 1(a): Benefits of different cloud service models.

SaaS [10]	PaaS [10]	IaaS [10]
i. Releases CSUs from application buying and maintenance cost. ii.Due to the use of World Wide Web it is easily accessible. iii. The service is reliable and CSU needs to pay only as much as they use. iv. CSU do not need to worry about the security issues. v. Cloud service users do not need spend time or money for complex installation of the applications and supporting hardware for them.	i. Facilities advantages, disadvantages and security issues of PaaS are quite similar with SaaS. ii. PaaS differs from SaaS in following two scenarios. a. Some PaaS are used for general development they do not depend upon any specific application. b. Some PaaS environment is used of security and on-demand scalability.	i. Infrastructure cost is a big issue for the young organizations. IaaS provides solutions in this area of problem. ii. The CSPs provide data availability, data security and maintenance of the infrastructure. iii. CSUs can access their data using some standard communication protocol or some standard security mechanism.

Table 1(b): Draw Backs of different cloud service models.

SaaS [10]	PaaS [10]	IaaS [10]
i. Some specific applications may not be found at the cloud. In that case the CSU may need to pick up the burden of buying and maintaining the application. ii. There is no standard or universal way of designing the SaaS cloud. This makes the application switching between two different clouds quite difficult. iii. Some time the service may be unavailable, due to the use of lower quality hardware by the CSPs or some sort of communication failure. iv. The encryption mechanism provided by the CSPs might not just be enough.	It has same draw backs as SaaS.	i. IaaS allows CSUs to run some software or applications in the CSPs infrastructures. This facility brings all the vulnerabilities associated with the Software or applications. ii. Many IaaS system supports auditing and Virtual Machine (VM) facilities for the ensuring the consistence of the data. If any of these facilities becomes vulnerable then the entire security of the cloud is compromised.

Table 1(c): Security issues of different cloud service models.

SaaS [10]	PaaS [10]	IaaS [10]
i. Strong data protection mechanism (e.g. encryption, steganographic approach) must be provided to secure the data. ii. The client side applications should also be protected.	PaaS have same security issues as SaaS. Along with the following issue. i. The platform support provided for developing the application should be generic so that it does not depend on any specific platform.	i. When IaaS is used for computing purpose in form of VMs. It may face security threats from other VMs of the same physical location or some other network threats. This can be solved by Virtual Firewall, Virtual IDS/IPS, and Virtual Private Networks. ii. A strong information security mechanism can be used for data protection. iii. Access over the out sourced data need to be controlled.

Due to cost effectiveness, availability, less maintenance burden many IT industries are moving towards cloud. But before moving on the cloud lets concentrate on the advantage [10] and disadvantage [10] of cloud.

Advantage:

i. Cost Effectiveness: Industries most of the expenditure increases for buying and maintaining software and infrastructure. Say a company needs to use some particular software once in a while, for that reason the company needs to buy the product, update the product and after some time the company needs to renew the license agreement. Cloud is the perfect remedy for this kind of increasing expenditure by its pay-as-use [10], one-time-payment etc.

ii. Scalability: This facility [10] basically supports the hardware problems. Due to this facility the Cloud service users never need to worry about the RAM, CPU usage or availability of disk storage space.

iii. Accessibility: Use of internet makes the cloud easily accessible anytime anywhere [10].

iv. Faster Deployment: This facility [10] makes the cloud services faster depending upon the type of service purchased and utilization.

v. Less Maintenance Burden: CSUs do not need to take the burden of installing [10] new software. They just need to select the suitable software or services.

vi. Backup and Recovery: As all the data is stored in the cloud, the CSU need not worry about the backup and recovery [10] of the data if any failure occurs.

Disadvantage:

i. Security: As the data is out sourced from local environment to cloud, the control of data is also transferred from CSU to CSP and as all the data of different organization resides in a single physical environment, the vulnerability of the data increases. So the CSUs depends upon heavily on the trust and security [10] mechanism of the CSPs.

ii. Internet Connectivity: The availability of entire cloud service depends on the communication internet connection [10]. If the connection fails then the service becomes unavailable. The inter connecting communication must be a secure connection because unsecure connections will bring more vulnerabilities to the cloud.

iii. Technical Issues: The technical problems [10] in the CSPs infrastructure may result in hours of unavailability of the data and this failure may also bring some serious damage or security threats to the outsourced data.

Cloud Service Agreement:

This is basically a legal aspect used for ensuring rights of the CSUs and CSPs. This is basically achieved by two parts [10] a) service agreement b) service level agreement. Service agreement specifies legal contract between CSUs and CSPs. Service Level Agreement (SLA) includes promises for technical performance and solutions for technical failures.

SLA can internally be used between the information systems units and other organization units just to ensure the alignment between the provided information technology services and the mission objectives.

A Service agreement has four parts a) Promises b) Limitations c) Obligations d) Recommendation.

a. Promises: This is phenomena [10] basically the promises made by the CSPs to the CSUs. These promises are mostly made on the following fields.

i. Availability: Most of the CSPs claim that their systems [10] are up for 24x7x365 with at least 99% efficiency. This statistics are achieved by calculation over a long period. Like if a CSP promises that their system will be in use in 15 minutes and system goes down for 14 minutes then the system is 100% functional. And they do not count the system failure during the time period when the services are not in use. CSPs may also hide the nonfunctional VMs just to make the statistics better.

ii. Remedies for the failures: If a CSP fails to provide proper performance then it must compensate the CSU for their failure [10].

iii. *Data preservation:* If a CSU stops using cloud [10] or the service of the CSU is terminated then the CSP alerts that the data will be deleted within certain period of time. The CSP may preserve a snapshot of the data or recommend the CSUs to move to another cloud or take a local backup.

iv. *Legal aspect of CSU information:* CSPs are strictly restricted [10] to outsource the CSUs data without their concern, but they may monitor CSUs data.

b. Limitations: the promises which are not made to the CSUs [10].

*i. Security: C*SPs deny any kind of security [10] issue, as none of the SLA discuses about the security issues. Few CSPs makes some promises about their security mechanism but some time it is proven to be inadequate.

ii. Service Agreement Changes: CSP reserves the right to change [10] the terms of service agreement without proper prior notice.

iii. *Scheduled Outages:* The scheduled service outages [10] by the CSPs are not considered as a failure.

iv. *Force major events:* CSPs do not take responsibilities for event out of their [10] control like natural disaster, power failure, network failure etc.

v. Service Interface changes: CSPs may change the Application Programming Interfaces [10] any time without any prior announcement.

c. Obligations: The problems mostly faced and accepted by the CSUs [10].

i. Acceptable Use Policies: CSUs are restricted from storing illegal [10] data in the cloud.

ii. Licensed Software: All CSPs claims that they use licensed third party software [10].

iii. *Timely Payment*: Cloud service costs are increasing gradually [10]. And the CSUs need to pay the money within a specific period of time otherwise this payment failure may result in discontinuation of the service.

d. Recommendations:

Terminology: CSUs must be make their selves clear about all the terminologies [10] no matter how common the term is.

i. Remedies: CSUs must negotiate about the security issues [10] in the service agreement.

ii. Compliance: CSUs should compliance [10] with appropriate laws and regulation related to consumer data

iii. Security and Availability: CSUs must be sure about the Security, fault tolerance, failure recovery mechanisms [10] provided by the CSPs.

iv. Negotiated Service Agreement: CSU must ensure that the service agreements [10] are ensuring all of its needs.

v. Service Agreement Changes: For any changes in the service agreement [10] the CSPs must come with a proper prior notice. These changes may affect both price and quality of the services.

In the next section authors have described the security threats and scheduling concerns of cloud service, followed by the existing solutions of the security and scheduling issues, analysis pros and cons and some remedies of the existing solutions, and the last section draws the conclusion on the paper.

Security Threats and Scheduling Algorithms

The two main features of cloud computing is "pay-per-use" and "multi tenancy" brings the two major problems for the cloud i.e. cloud computing security threats and scheduling problem. Fig 2 and 3 illustrates the survey report conducted by International Data Corporation (IDC) [11], which enlightens the concern for proper security and proper scheduling in cloud. In both 2008 and 2009 security and scheduling (together availability and performance) are the major concerns.

Security Threats

The cloud computing security issues are guided by the International Standards Organization (ISO) 7498-2 [12] . Fig 4, describes the different security threats of different types of cloud services [13]. In Fig 4 "+" means mandatory requirement and "-" means optional requirements.

The security requirements are described bellow in context of cloud computing.

Identification & Authentication

This security requirement deals with access control in the cloud. It aims at authenticating and validating each cloud service users (CSU). This may require user id, password or some other authenticating mechanisms [12].

Authorization

It ensures [12] the referential integrity. It controls process flow or service flow in a cloud. This security requirement is basically maintained by the cloud service providers (CSP).

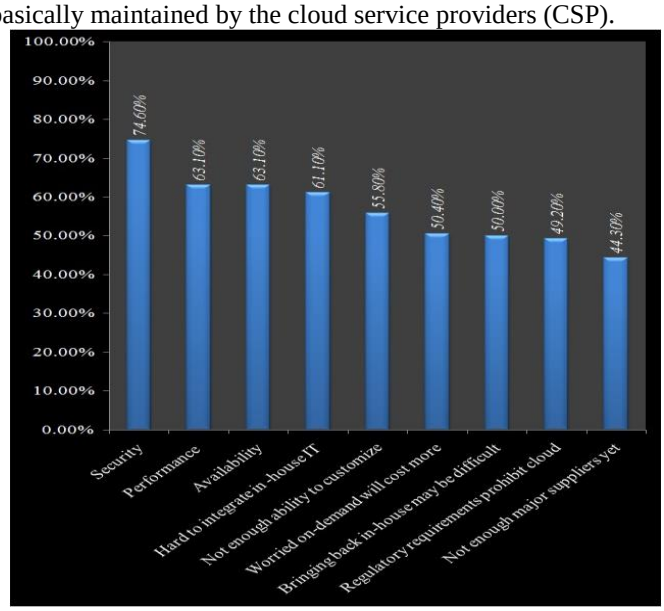

Fig 2: Cloud challenges/issues survey 2008 (n=244) (in courtesy International Data Corporation (IDC) [11])

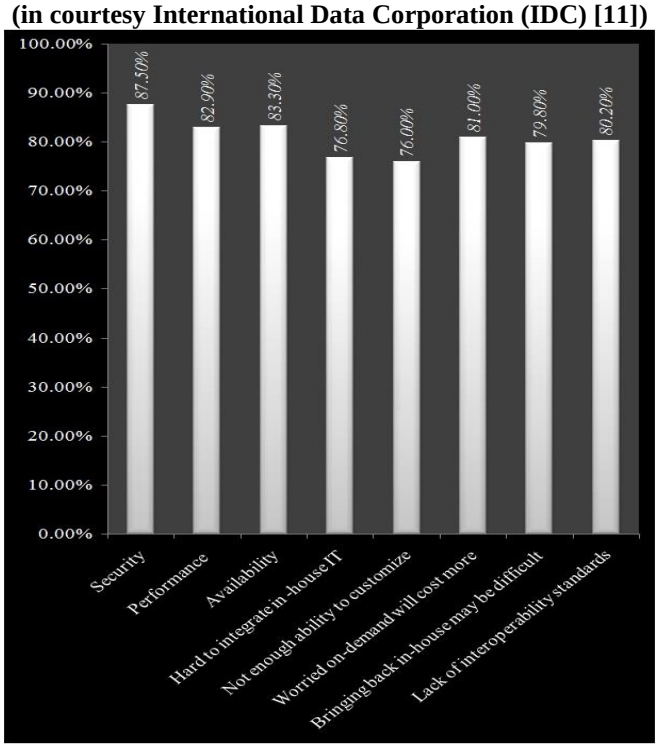

Fig 3: Cloud challenges/issues survey 2009 (n=263) (in courtesy International Data Corporation (IDC) [11])

Confidentiality

Confidentiality [12] ensures that, unauthorized parties are prevented from obtaining private information. To maintain the multi tenancy as well as security of a cloud this feature plays a vital role. Virtual accessing of data allows maintaining the confidentiality to some extent.

Integrity

The integrity [12] describes about the requirements to protect components of the system from intentional and unauthorized harm. Integrity requirements can be classified in data integrity, hardware integrity and software integrity. In many of the cases it is achieved by service level agreements.

Non-repudiation

Non-repudiation [12] ensures that none of the communicating parties can deny (repudiation) the communication between them. Repudiating interactions is often counteracted by preventing authorized access in the first place. These techniques are therefore often used for access control requirements. Amongst others, the exchange of public keys, certificates or signatures are included.

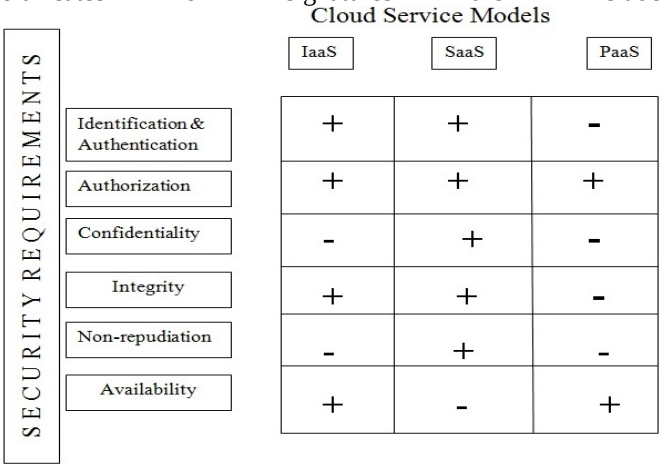

Fig 4: Cloud Computing Security Requirements

Availability

Cloud depends upon the types of services it provides. So for a cloud, availability [12] of the services is a major factor. It's a part of cloud security as well as cloud scheduling. This is can be dealt with some service level agreements (SLA) between CSP and CSU.

Scheduling

Cloud is "pay-per-use" service. So scheduling [14] of tasks plays a vital role for full utilization of services in a cloud. Various scheduling algorithms deal with this issue. But traditional job scheduling algorithms are unable to serve the purpose. Job scheduling algorithms can be classified into i) Batch mode heuristic scheduling algorithms (BMHA) and ii) online mode heuristic algorithms(OMHA). In BMHA jobs are collected in a set according to their arrival in the system and after certain time interval the scheduling algorithm will start. Like First Come First Served scheduling algorithm (FCFS), Round Robin scheduling algorithm (RR), Min–Min algorithm and Max–Min algorithm. And in case of OMHA jobs are scheduled according to their arrival in the system. This process is more effective than BMHA due to its heterogeneous nature of cloud where the speed of each processor varies quickly. Example Most Fit Task Scheduling algorithm (MFTS).

First Come First Served scheduling algorithm

The job is done by first come first serve basis [14]. This algorithm assigns the jobs in a ready queue according to their arrival. It's easy to implement but throughput is slow as the longer jobs may block the entire system for a long time.

Round Robin algorithm

The jobs are done in a first in first out (FIFO) [14] manner. Each job is assigned a limited amount of processing time which is called time-slice or quantum. If a job does not complete in a given time slice then it's placed at the end of the ready list and next job is placed for execution.

Min–Min algorithm

This is a static task scheduling algorithm [14]. The smallest job is executed at first. When the system is at idle state it checks for the smallest job and makes a queue depending upon completion time. In this algorithm the largest job's takes longest time. The smallest job's takes longest time. Time complexity of the algorithm is $O(mn^2)$ m is the number of available resources and n is the number of jobs.

Max – Min algorithm

This algorithm [14] is basically used in an environment where jobs are unscheduled in manner. It calculates expected execution time on the available resources. Then the job with longest execution time is executed at first followed by the shorter jobs. The smallest job's takes longest time. Time complexity of the algorithm is $O(mn^2)$ m is the number of available resources and n is the number of jobs.

Most fit task scheduling algorithm

In this algorithm [14] each job is assigned with a fitness value depending upon some predefined parameter. The jobs are placed in a ready queue according to their fitness values. The fittest job in the queue is executed first followed by the lower fitness value. But this algorithm has a high failure ratio.

Priority scheduling algorithm

This algorithm [14] each job is assigned with a priority. And each job is executed according its priority value, same priority jobs are executed according to FCFS basis. The Shortest-job-First (SJF) is the most popular way to assign priority to the jobs. The longest process is presented with lowest priority.

Existing Security and Scheduling Solutions

Existing security Solutions

Md.Tanzim Khorshed et al. [15] has proposed an attack is detection mechanism using machine learning mechanism and depending upon the pattern of the attack type of attack is identified and both the CSU and CSP's are informed. Figure 5 describes the working principal of the method. This solution can be useful for all the cloud models.

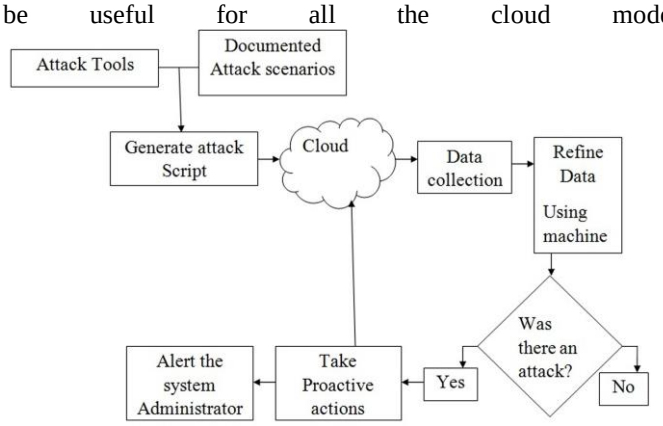

Fig 5: Attack detection and proactive resolution (In courtesy Md.TanzimKhorshed et al. [15])

For IaaS Environment

Cong Wang et al. [16] gives a method where an external auditor audits the users out sourced data in the cloud of behalf of the user depending upon some authentication key. This method also supports batch auditing i.e. Third party Auditor (TPA) can simultaneously perform auditing for different users.

Xiaojun Yu et al.'s method [17] data is encrypted in storage. In here authors have use asymmetric cryptography at the storing phase of data. Figure 6 describes the working principal of the model.

Uma Somani et al. [18] have used RSA, for secure transmission of data over the network and digital signature signifies the authenticity of data, in a mathematical form. This form is provided by "hashing algorithm", which will transfer the data into message digest.

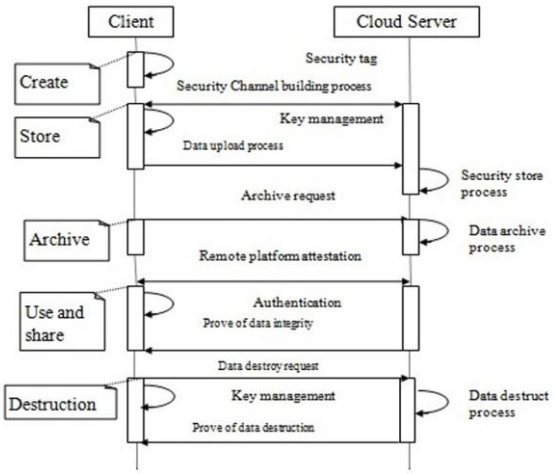

Fig 6: Data security process in data life cycle (in courtesy Xiaojun Yu et al. [17])

P. Syam Kumar et al. [19] have proposed an effective and flexible distribution verification protocol to address IaaS model of cloud. This method uses erasure code for data availability, reliability. Utilize token pre-computation using sobel sequence to verify integrity of erasure coded data rather than pseudo random data in existing system. For better availability of data, entire data is distributed among "N" no. of sites and if few sites fails among N, then also the original data can be retrieved from the remaining sites. This makes the system fault tolerant.

For SaaS and PaaS

Xi Cao et al. [20] have proposed a two way security protocol.

Step1. CSP obtain the signature of CSU's to confirm the cloud service.

Step 2. Software provider obtains the signature CSP's to count the number of service.

During cloud service interaction disputes like repudiation and impersonation may occur. Figure 7 describes the working principal.

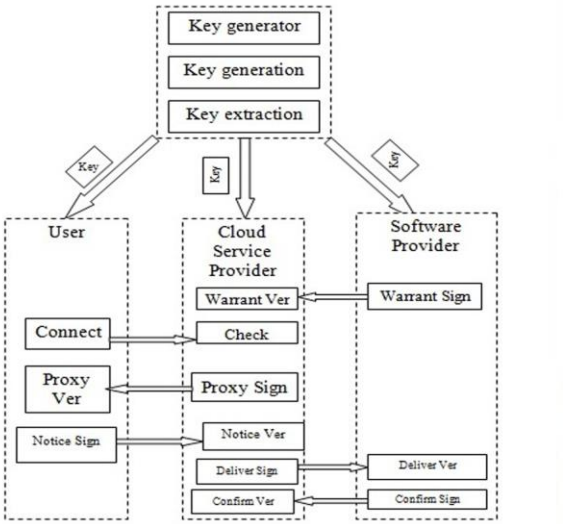

Fig 7: Id-based proxy Signature Model for cloud service in Saas(In courtesy Xi Cao et al. [20])

Junli Zhu et al. [21] have developed a security system over the UCON model. This model consists of total eight components subject, subject attributes, object, object attributes, rights, authorization, obligations and conditions. Figure 8 describes the detail of the process.

Kiyoshi Nishikawa et al. [22] method security is achieved through information gateway that enables cloud service while maintaining confidentiality by setting up information gateway in the client environment. The executing location is dynamically controlled according to whether the data contains confidential information or not and only secured data is routed to the SaaS application in the cloud.

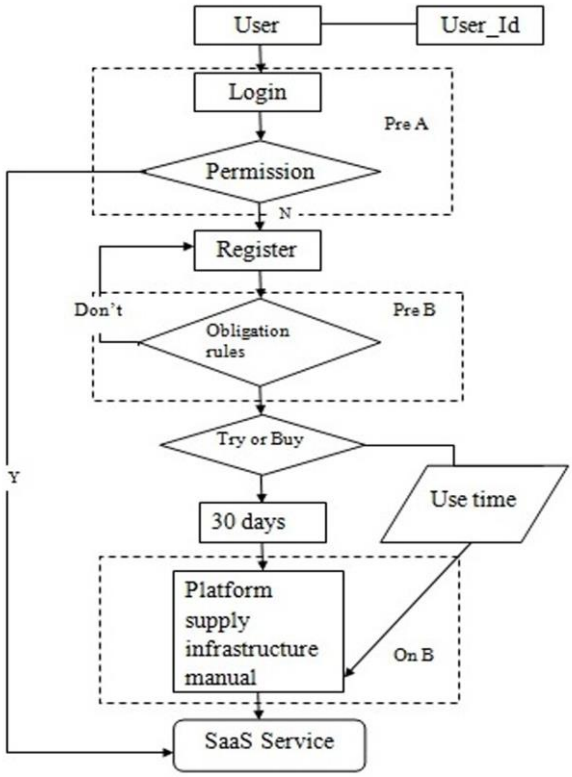

Fig 8: UCON Combined with SaaS Access Flow (In courtesy Junli Zhu et al. [21])

Some other Security Solutions

Jinpeng Wei et al. [23] Proposes a model to manage the virtual machine image in a cloud environment in secure manner.

Disadvantage: The image filters cannot be accurate so that system does not eliminate the risk entity.

Miranda Mowbray et al. [24] Proposes a client based privacy manager for reducing the risk of misuse the user's private data and also assist the cloud computing provider to confirm the privacy law.

Disadvantage: The service providers have to provide honest cooperation with the privacy manner or it's not an effective one.

Flavio Lombardi et al. [25] uses Transport Cloud Protection System (TCPS) as a middle ware whose core is located between kernel and virtualization layer.

Advantage: Effecting in detecting most kind of attacks.

Disadvantage: This is not generalized one it cannot be implemented in all seniors.

F. A. Alvi et al. [26] have developed a security access control service (SACS) model modeled to improve security in cloud data.

Disadvantage: Still unknown killer application cannot be avoided.

Shantanu Pal et al. [27] proposed a trust based agent frame work which provides security at service provider level and use level in cloud environment.

Disadvantage: It can handle limited amount of security threats.

Existing Scheduling Solutions

Saeed Parsa et al. [28] have proposed a new task scheduling algorithm based on advantages of Max-Min and Min-Max. This process does not consider arriving rate, execution cost and communication costs. The experimental result shown by the author leaves other methods far behind.

Arash Ghorbannia Delavar et al. [29] have sub divided a major jobs into smaller sub jobs. Sub job request and acknowledge time is calculated separately to maintain balance. Each job is scheduled by calculating the request and acknowledgement time in the form of a shared job to increase the efficiency of the system.

Dr. M. Dakshayini et al. [30] have done the scheduling by priority and admission control scheme. In here priority is assigned to each admitted queue. Tolerable delay and service cost is decides the admission of each queue. This method has achieved very high service completion rate. Overall service cost may increase as the service provides highest precedence for highly paid user service-request.

Shamsollah Ghanbari et al. [31] have proposed a new scheduling algorithm based on multi-criteria and multi-decision priority .This contains three levels of scheduling. Priority is assigned according to job resource ratio. Then priority vector is compared with each queue.

El-Sayed T. El-kenawy et al. [32] proposed a scheduling algorithm which is based on Saeed Parsa et al.'s [28] Max- Min and Min-Max method. El-Sayed T. El-kenawy et al. [32] have improved Max-Min. Here execution time is considered instead of complete time as a selection basis. It consists considerably smaller make span rather than Saeed Parsa et al.'s [28].

Shalmali Ambike et al. [33] have done scheduling by non-preemptive priority queuing model depending on activities performed by cloud user in the cloud environment. This algorithm requires a web application which uploads, downloads some files for effective job scheduling.

Mrs.S.Selvarani et al. [34] uses an efficient mapping of jobs to available recourse in cloud. This is a cost-based scheduling. This scheduling algorithm divides all jobs depending on priority of each job into three different lists. It measures both resource cost and computation performance.

Detail Analysis Of Existing Solutions

Pros and cons of the existing solutions

In this section authors have tried to highlight the advantages and disadvantages of the existing security solutions, where Table 2(a) deals with IaaS environment and Table 2(b) with PaaS and SaaS environment.

Table 2(a): Pros and Cons of existing security solutions for IaaS environment

Security algorithm	Pros	Cons
By Md.TanzimKhorshed et al. [15] **(This solution is applicable for all type of cloud service models)**	i. Activities are detected from the hyper version and its guest operating system, so user doesn't rely on CSP's security log or data	i. Fewer no of attacks can be detected. i. Use of large data bases for machine learning makes the attack detection slower.
By Cong Wang et al. [16]	i. The process is scalable, with efficient public auditing. ii. It supports Batch auditing. iii. It reduces the auditing burden to the cloud user.	i. If TPA becomes vulnerable the entire security of the cloud is compromised. ii. Use of many "Batche auditing" at a single time makes the TPA harder to track. iii. Excessive use of batch auditing may result into a system crash. iv. If the non legitimate user steels the data not by destroying the original data, then it remains undetected to the auditor. v. Number of keys limits the no of auditing of a particular file. So after using all the keys user needs to audit the file manually.
By Xiaojun Yu et al.'s method [17]	i. Very easy to implement. Any conventional encryption procedure will do the trick.	i. No auditing facility.
By Uma Somani et al. [18]	i. RSA is a well known asymmetric key cryptographic method which will provide the security of data. ii. Digital signature ensures data authenticity.	ii. To check the integrity of the data user have to download the whole data, which will make the communication cost huge.
By P. Syam Kumar et al. [19]	i. User copy is not required to verify of the data. ii. TPA may provide security in various levels. iii. The system is fault tolerant. iv. Effective against Byzantine failure, unauthorized data modification attacks and even cloud server colluding attack.	i. As the file becomes larger the pre-computed values also becomes larger. ii. Only the responses from servers are not enough for identifying misbehavior of data. iii. Due to adding extra erasure code total space over head may be increased.

Table 2(b): Pros and Cons of existing security solutions for PaaS and SaaS environment

Security algorithm	Pros	Cons
By Xi Cao et al. [20]	i. Suitable against DOS attack.	i. The key generation phase and both way communication between three sites, results huge communicational cost and computational cost for CSPs. ii. If the software provider site becomes faulty then CSP cannot provide proper service. iii. Except DOS attack it's not that much effective.
By Junli Zhu et al. [21]	i. Good as a Authentication Protocol.	i. It does not take necessary steps for DOS attack, confidentiality etc.

Analysis of Scheduling Solutions

Table 3 describes details of the Scheduling solutions.

Table 3: Details of the scheduling solutions

Scheduling Algorithm	Scheduling Mode	Scheduling Parameters	Scheduling Factors	Advantages
By Saeed Parsa et al. [30]	Batch mode	Max-Min and Min-Max	Set of jobs	i. Reduces waiting time for jobs
By Arash Ghorbannia Delavar et al. [29]	Batch mode	Jobs divided in Sub jobs	Set of jobs	i. Reduces processing time ii. Efficient load balancing
By Dr. M. Dakshayini et al. [30]	Batch mode	QOS , service request time to calculate priority	Jobs are admitted according to priority	i. High QOS ii. High throughput
By Shamsollah Ghanbari et al. [31]	Dependency Mode	Priority to each queue	Array of job	i. Faster than other methods.
By El-Sayed T. El-kenawy et al.'s [32]	Batch mode	Load balancing	Set of jobs	i. Efficient load balancing ii. Improves max-min algorithm

By Shalmali Ambike et al. [33]	Dependency Mode	QOS	One job many user	i. QOS for the CSU and max profit for CSP
By Mrs.S.Selvarani et al. [34]	Batch mode	Cost effective and efficient	Unscheduled jobs	i. Measures both cost and efficiency ii. Improved computation, commu--nication ratio.

Some Proposed Solutions

For IaaS:

Depending upon Cong Wang et al.'s [16]

i. The number of batch auditing must be controlled.

ii. The auditing protocol used should be lighter otherwise it may lead to high computational overhead.

iii. The system should be equipped to track each access of data. So that if the TPA becomes vulnerable then the system could be able to track it down.

iv. TPA must not become vulnerable in any circumstances.

For Xiaojun Yu et al.'s [17] and Uma Somani et al.'s [18]

i. Symmetric key or asymmetric key cryptography may bring communication overhead for the CSUs to check the data integrity. So homomorphic Encryption [35] can be used instead of symmetric key or asymmetric key cryptography.

ii. TPA must be able to maintain data integrity. So that the CSUs can be sure about their data.

For SaaS and PaaS:

For Xi Cao et al.'s [20]

i. Separate verification between CSU and CSP only increases computational and communicational overhead. So, the same verification can be done between user and CSP at the time of service request, with lesser computational and communicational cost.

ii. Separate key generation mechanism for each site is not necessary. To avoid DOS attack, one simple notification at the end of each task, is enough.

iii. DOS is not the only threat SaaS and PaaS usually face. So other threats should also be considered.

For Kiyoshi Nishikawa et al.'s [21] and Jinpeng Wei et al.'s [22]

i. The system is not equipped to deal with all kinds of threats. So, it should be updated to deal with all kind of attacks.

Conclusion

Moving towards cloud is the current trend of the IT industries due to its cost effectiveness and accessibility. Like many other new technologies cloud computing has a potential to make human life better. But one must be understand the limitations and security issues associated with every new technology. Cloud is no exception.

In this paper authors have concentrated on different key aspects of cloud, like security aspect, scheduling aspect, legal aspect including their existing solutions. The authors have also discussed the pros and cons of the existing solutions. Due to complex nature of the cloud its quite difficult to fill all the gaps of the existing solutions. So new solution systems must be or the gaps of the existing solutions are to be filled as described in this paper developed to make the cloud more efficient.

References

[1] P. Mell, T. Grance, NIST definition of cloud computing. National Institute of Standards and Technology, October 2009

[2] GTSI Group, "Cloud Computing - Building a Framework for Successful Transition," *White Paper, GTSI Corporation, 2009.*

[3] Grace A. Lewis Research, Technology and Systems Solutions (RTSS) Program "Architectural Implications of Cloud Computing", May 18, 2011

[4] http://en.wikipedia.org/wiki/Cloud_computing

[5] "Recession Is Good For Cloud Computing – Microsoft Agrees".CloudAve. Retrieved 2010-08-22.

[6] "e-FISCAL project", http://www.efiscal.eu/state-of-the-art

[7] Farber, Dan (2008-06-25). "The new geek chic: Data centers". CNET News. Retrieved 2010-08-22.

[8] King, Rachael (2008-08-04). "Cloud Computing: Small Companies Take Flight". Business week. Retrieved 2010-08-22.

[9] "The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 2011.

[10] Book: "Information Security' by D.P.Nagpal by S.Chand Publisher.(S.Chand & Company Pvt Ltd)

[11] Gens F, 2009,' New IDC IT Cloud Services Survey: Top Benefits and Challenges', IDC eXchange, viewed 18 February 2010, from <http://blogs.idc.com/ie/?p=730>.

[12] ISO. ISO 7498-2:1989. Information processing systems-Open Systems Interconnection. ISO 7498-2

[13] Dlamini M T, Eloff M M and Eloff J H P, 'Internet of People, Things and Services – The Convergence of Security, Trust and Privacy', 2009

[14] Pinal Salot , "A Survey Of Various Scheduling Algorithm In Cloud Computing Environment", Volume: 2 Issue: 2, 131 – 135, ISSN: 2319 - 1163

[15] Md.TanzimKhorshed,A.B.M.ShawkatAli,SalehA.Wasimi," Asurveyongaps,threatremediationchallengesandsomethoughtsfor proactive attack detection in cloud computing", *School of Information and Communication Technology, CQ University QLD4702, Australia*

[16] Cong Wang, Qian Wang, and Kui Ren Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", *IEEE INFOCOM 2010*

[17] Xiaojun Yu, Qiaoyan Wen, "A View About Cloud Data Security From Data Life Cycle", *IEEE ,2010*

[18] Uma Somani, Kanika Lakhani, Manish Mundra , "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" , *2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010)*

[19] P. Syam Kumar, R. Subramanian and D. Thamizh Selvam, "Ensuring Data Storage Security in Cloud Computing using Sobol Sequence", *2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC – 2010) ,IEEE.*

[20] Xi Cao, Li Xu, Yuexin Zhang and Wei Wu, "Identity-based Proxy Signature for Cloud Service in SaaS", *Fourth International Conference on Intelligent Networking and Collaborative Systems, 2012*

[21] Junli Zhu, and Qiaoyan Wen,"SaaS Access Control Research Based on UCON*", Fourth International Conference on Digital Home, 2012*

[22] Kiyoshi Nishikawa, Kenji Oki and Akihiko Matsuo, "SaaS Application Framework using Information Gateway Enabling Cloud Service with Data Confidentiality", *19th Asia-Pacific Software Engineering Conference,IEEE, 2012.*

[23] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala,peng Ning."Managing Security of virtual machine images in a cloud environment ".*CCSW'09: Proceedings of the 2009 ACM workshop on Cloud computing security, November 2009, pp 91-96.*

[24] Miranda Mowbray, Siani Pearson "A Client –based privacy Manager for Cloud Computing*". OMSWARE '09: Proceedings*

of the Fourth International ICST Conference on communication system software and middle ware, June 2009.

[25] Flavio Lombardi, Roberto Di Pietro. "Transparent Security for Cloud". *SAC '10: Proceedings of the 2010 ACM Symposium on Applied Computing, March 2010, pp 414-415.*

[26] F. A. Alvi, B.S Chaudhary," review on cloud computing security issues &challenges".

[27] Shantanu Pal, Sunirmal Khatua, Nabendu Chaki, Sugata Sanyal, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security", *Annals of Faculty Engineering Hunedoara International Journal of Engineering (Archived copy), scheduled for publication in vol. 10, issue 1, January 2012. ISSN: 1584-2665.*

[28] Saeed Parsa and Reza Entezari-Maleki, " RASA: A New Task Scheduling Algorithm in Grid Environment*" in World Applied Sciences Journal 7 (Special Issue of Computer & IT): 152-160, 2009.Berry M. W., Dumais S. T., O'Brien G. W. Using linear algebra for intelligent information retrieval, SIAM Review, 1995, 37, pp. 573-595.*

[29] Arash Ghorbannia Delavar,Mahdi Javanmard ,Mehrdad Barzegar Shabestari and Marjan Khosravi Talebi "RSDC (RELIABLE SCHEDULING DISTRIBUTED IN CLOUD COMPUTING)" *in International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.3, June 2012*

[30] Dr. M. Dakshayini, Dr. H. S. Guruprasad "An Optimal Model for Priority based Service Scheduling Policy for Cloud Computing Environment*" International Journal of Computer Applications (0975 – 8887) Volume 32– No.9, October 2011*

[31] Shamsollah Ghanbari, Mohamed Othman "A Priority based Job Scheduling Algorithm in Cloud Computing" *International Conference on Advances Science and Contemporary Engineering 2012 (ICASCE 2012)*

[32] El-Sayed T. El-kenawy, Ali Ibraheem El-Desoky, Mohamed F. Al-rahamawy "Extended Max-Min Scheduling Using Petri Net and Load Balancing" *International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-4, September 2012*

[33] Shalmali Ambike, Dipti Bhansali, Jaee Kshirsagar, Juhi Bansiwal " An Optimistic Differentiated Job Scheduling System for Cloud Computing" *International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2,Mar-Apr 2012, pp.1212-1214*

[34] Mrs.S.Selvarani; Dr.G.Sudha Sadhasivam, "improved cost-based algorithm for task scheduling in Cloud computing" ,*IEEE 2010.*

[35] http://en.wikipedia.org/wiki/Homomorphic_encryption