International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Cloud Computing Security Issues and Control Mechanisms

Shital B. Patil[1], Dr. Shashi U. Ghumbre[2]

[1, 2]Computer Engineering Department, College of Engineering, Pune, Maharashtra India

Abstract: ***In cloud computing services, security and privacy concerns are like those of traditional non-cloud services, concerns are amplified by outer control over organizational resources and the potential for mismanagement of those resources. Transitioning to public cloud computing includes an exchange of responsibility and control to the cloud provider over data and system components that were already under the organization's direct control. The transition is normally accompanied by loss of direct control over the management of operations furthermore a loss of impact over decisions made about the computing environment. Regardless this underlying loss of control, the cloud service consumer still needs to take responsibility for their utilization of cloud computing services to keep up situational awareness, measure choices, set needs, and impact changes in security and privacy that are to the greatest advantage of the organization. The consumer attains to this by guaranteeing that the contract with the provider and its related Service Level Agreement (SLA) has proper provisions for security and privacy. Specifically, the SLA must help keep up legal protections for security identifying with information stored on the provider's system. The consumer must also ensure proper integration of the cloud computing services with their own systems for managing security and privacy.***

Keywords: cloud computing, privacy, security, service level agreement (SLA).

1. Introduction

Cloud computing changes the way in which current enterprises IT base is constituted and managed through consumable services, for example, framework, platform, and applications. It will change over the IT framework from a "manufacturing plant" into a "supply chain" model. It is a sort of computing that gives simple, on-demand access to pools of highly elastic computing resources [1]. These resources are given as a service over a network, frequently the Internet. Cloud empowers the consumers of the technology to consider computing successfully boundless, of insignificant expense, and reliable, and also not to be worried about how it is developed? How it functions? Who works it? Or where it is placed? The cloud computing model [4,5] is empowered by the progressing standardization of underlying technologies like virtualization, Service Oriented Architecture (SOA), and Web 2.0. Cloud computing is a style of computing where computing resources are not difficult to acquire and access, easy to utilize, cheap, and simply work. Cloud is not a point item or a singular technology, yet an approach to convey IT resources in a way that gives organization toward oneself, on-demand and pay-per-use utilization. Using cloud conveys time and cost savings. Cloud includes the subscriber and the provider. The service provider can be a company's inside IT group, a trusted outsider or a mix of both. The subscriber is any individual who utilizes the services. By making information accessible in the cloud, it can be all the more effortlessly and pervasively accessed, regularly at much lower expense, expanding its esteem by empowering opportunities for improved collaboration, integration, and an analysis on an imparted basic platform.

2. Types of Cloud

In a cloud computing framework, there's a significant workload shift. Local computers no more need to do all the heavy lifting with regards to running applications. The network of computers that form the cloud handles them rather which leads in reduction of hardware and software requests on the client's side. The main thing the client's computer needs to have the capacity to run is the cloud computing frameworks interface software, which can be as basic as a Web browser, and the cloud's system deals with the rest. There are three common types of clouds accessible to be specific, Private, Public and Hybrid cloud. A private cloud is based upon a pool of shared resources, whose right to gain access is restricted inside organizational limits. The resources are accessed over a private and secured intranet, and are all possessed and controlled by the company's IT organization. Fundamentally, the cloud computing business model[6] is gotten and managed in-house to empower shared IT services. A public cloud is a domain where the public Internet is utilized to get cloud services. The resources that form those services are possessed by the particular cloud service providers. A few samples incorporate Salesforce.com, Google App Engine and Google look, Microsoft Azure, and Amazon Web services such as Ec2. A Hybrid cloud is a combination of private and public clouds, where services from every space are consumed in an incorporated manner and include an amplified association with the selected outer service providers.

1) Cloud Computing Service Model

Private and Public clouds serve as the backbone for an assortment of distinctive cloud computing service models. At present the business has been effectively receiving three normal sorts of cloud computing service models. Infrastructure-as-a-Service (Iaas), is a service demonstrate around servers (compute power), storage capacity, and system data transfer capacity[10]. Samples incorporate Amazon Ec2 and S3, Rackspace, AT&T, and Verizon. Platform-as-a-Service (Paas) gives a remotely managed platform for building and deploying applications and services. This model ordinarily gives development tools[11], for example, databases and development studios for working

with the supplied systems, and in addition the framework to host the built application. Examples are SalesForce.com, Microsoft Azure, and Google App Engine. Software-as-a-Service (Saas) is basically having a software framework running on a computer that doesn't fit in with the client and isn't on the customer's premises. It is focused around the idea of leasing an application from a service provider instead of purchasing, installing and running programming yourself.

2) Advantages of Cloud Computing

Cloud computing offers the following advantages to the ventures:

- *Lower costs*: All resources, including costly systems equipment, servers, IT staff, and so forth are shared, bringing about diminished expenses, particularly for small to mid-sized applications.
- *Shifting Capital Expenses to Operational Expenses*: Cloud computing empowers organizations to move cash from capital costs to working costs, which eventually permits the venture to center their cash and resources on advancement.
- *Agility*: Provisioning on-demand empowers quicker setup on an as-required premise. At the point when a project is financed, client can launch service, and after that if the project is over, they can just end the cloud contract.
- *Scalability:* Many cloud services can easily and proficiently scale to handle the becoming nature of the business with a more cost effective pay-as-you-go model. This is otherwise called elasticity.
- *Simplified support:* Patches and updates are quickly conveyed over the shared base, and additionally the reinforcements.
- *Diverse platform support:* Many cloud computing services offer implicit backing for a rich accumulation of customer platforms including browsers, mobile, and that's just the beginning. This differing platform backing empowers applications to achieve a more extensive classification of clients.
- *Faster development:* Cloud computing platforms give many of the core services that, under conventional advancement models, would regularly be built in house. These services, in addition to layouts and different tools can essentially quicken the development cycle.

3. Security issues in cloud computing

At the present time, cloud computing makes up a very dynamic area with new providers and new offerings arriving constantly. There are various security risks connected with cloud computing that must be satisfactorily tended to:

- *Loss of administration:* For public cloud arrangements, consumers fundamentally cede control to the cloud provider over various issues that may influence security. In the meantime, cloud service level agreements (SLA) may not offer a guarantee to give such abilities from the cloud provider, in this way leaving holes in security safeguards.
- *Responsibility equivocalness:* Given that utilization of cloud computing services compasses over the consumer and the provider organizations, responsibility regarding parts of security can be spread crosswise over both organizations, with the potential for key parts of the safeguards to be left unguarded if there is an inability to allot responsibility clearly. The part of responsibilities in the middle of consumer and provider organizations is liable to differ relying upon the model being utilized for cloud computing (e.g. Iaas versus Saas).
- *Isolation failure:* Multi-tenancy and shared resources are characterizing attributes of public cloud computing. This risk class covers the disappointment of components dividing the utilization of capacity, memory, routing and even reputation between different tenants (e.g., so-called guest-hopping attacks).
- *Vendor lock-in:* Dependency on restrictive services of a specific cloud provider could lead to consumer being attached to that provider. Services that don't help portability of applications and information to different providers increase the risk of information and service inaccessibility.
- *Compliance and legal risks*: Investment in achieving certification (e.g., industry standard or administrative prerequisites) may be put at risk by movement to utilize cloud computing if the cloud provider can't give confirmation they could call their own consistence with the applicable necessities or if the cloud provider does not allow audit by the cloud consumer. It is the responsibility of the cloud consumer to watch that the cloud provider has appropriate certifications set up, yet it is additionally essential for the cloud consumer to be clear about the division of security responsibilities between the consumer and the provider and to guarantee that the consumer's responsibilities are taken care of properly when utilizing cloud computing services.
- *Handling of security occurrences*: The discovery, reporting and resulting administration of security breaches is a concern for consumers, who are depending on providers to handle these matters.
- *Management interface vulnerability:* Consumer administration interfaces of a public cloud provider are generally available through the Internet and mediate access to bigger sets of resources than conventional facilitating providers and hence represent an expanded risk, particularly when consolidated with remote access and web browser vulnerabilities.
- *Data assurance:* Cloud computing represents a few information security risks for cloud consumers and providers. The real concerns are introduction or release of sensitive information additionally incorporate loss or inaccessibility of information. Sometimes, it might be difficult for the cloud consumer (in the part of information controller) to adequately check the information handling practices of the cloud provider and in this way to make sure that the information is handled in a legitimate manner. This issue is exacerbated in instances of multiple transfers of information, e.g., between federated cloud services.
- *Malicious behavior of insiders:* Harm brought about by the malicious activities of insiders working inside an organization can be significant, given the right to gain the access and approvals they may have. This is aggravated in the cloud computing environment since such action may happen inside either or both the consumer and the provider organizations.
- *Service inaccessibility:* This could be brought on by a host of factors, from equipment or programming failures in the provider's data center, through failures of the interchanges

between the consumer frameworks and the provider services.

- *Insecure or fragmented information erasure:* Solicitations to erase cloud resources, for instance, when a consumer ends service with a provider, may not bring about genuine wiping of the information. Satisfactory or timely information deletion might likewise be impossible (or undesirable from a consumer point of view), either on the grounds that additional duplicates of information are put away however are not accessible, or because the disk to be erased additionally stores information from different clients. On account of multi-tenancy and the reuse of H/W resources, this leads to a higher risk to the consumer than is the case with committed H/W.

While the above security risks need to be tended to, utilization of cloud computing gives chances to advancement in provisioning security services that hold the possibility of enhancing the general security of numerous organizations. Therefore, Cloud service providers should be able to have the capacity to offer advanced facilities for supporting security and privacy because of their economies of scale and automation capacities - conceivably a shelter to all consumer associations, particularly the individuals who have restricted numbers of personnel with advanced security skills.

4. Control Mechanisms

As consumers move their applications and information to utilize cloud computing, it is basically important that the level of security gave in the cloud environment be equivalent to or better than the security gave by their traditional IT environment. Inability to guarantee suitable security could eventually bring about higher expenses and potential loss of business hence eliminating with any of the potential advantages of cloud computing.

This section gives a prescriptive series of steps that should be taken by cloud consumers to assess and deal with the security of their cloud environment with the objective of moderating risk and conveying a appropriate level of support. The following steps are discussed in detail:

A. Ensure Effective Administration, Risk and Compliance Methodologies Exist

Most organizations have created security and compliance policies and methods that are utilized to secure their intellectual property and corporate resources particularly in the IT space. These policies and methods are produced based upon risk investigation to the organization considering the effect of having these assets compromised. A system of controls and further methods are built to moderate risk and serve as a benchmark for the execution and approval of compliance. These standards and policies, the enterprise security plan, and the encompassing quality change procedure represent the enterprise security administration, risk management, and compliance model.

The essential means a consumer of cloud service needs to guarantee their cloud hosted applications and information will be secured as per its security and compliance approaches is to check that the contract between the consumer and the provider, alongside a related service level agreement (SLA), contain all their prerequisites. It is vital for a consumer to see all the terms identified with security and to guarantee that those terms address the needs of the consumer. On the off chance that a suitable contract and SLA is not accessible, then it is inadvisable for an organization to move ahead with the utilization of cloud services.

Frequently it is not understood that the kind of service model being offered by the provider (i.e. Iaas, Paas or Saas) has noteworthy effect on the accepted "part of responsibilities" between the consumer and the provider to manage security and related risks. For Iaas, the provider is supplying (and in charge of securing) essential IT resources, for example, machines, disks and networks. The consumer is in charge of the operating system and the whole software stack important to run applications, in addition to the information placed into the cloud computing environment. Thus, the majority of the responsibility regarding securing the applications themselves and the information they utilize falls onto the consumer. Conversely, for Saas, the framework, software and information are basically the responsibility of the provider, since the consumer has little control over any of these features of the service. These angles need suitable handling in the contract and SLA.

From a general administration point of view, cloud providers should tell consumers about the event of any breach of their framework, despite of the parties or information specifically affected. The provider should incorporate specific pertinent information in the notification, stop the information breach as fast possible, restore secure access to the service as quickly as possible, apply best-practice forensics in investigation in exploring the circumstances and reasons for the breach, and roll out long-term base improvements to correct the underlying causes of the breach to guarantee that it doesn't repeat. Because of the high financial and representational expenses coming about because of a breach, consumers may need the provider to repay them if the breach was their fault.

One valuable methodology to the security difficulties of cloud computing is for a cloud provider to show that they are compliant with a made set of security controls. Accreditation of the provider gives more trust in that provider to prospective consumers. There are various different certifications which can be helpful for cloud computing services - which one is most suitable depends to some degree on the cloud service model (Iaas, Paas, Saas) furthermore relies on client's regional and industry requirements.

B. Audit and Guarantee Legitimate Reporting of Operational & Business Processes

Organizations understand the significance of auditing the compliance of IT frameworks, which have their applications and information, to evaluate effectiveness in authorizing their corporate, industry or government prerequisites and policies. As a standard, consumers should hope to see a report of the cloud provider's operations by independent auditors. Liberated access to essential audit data is a key consideration of contracts and SLA terms with any cloud provider. As a major aspect of any terms, cloud providers should offer auspicious access to and self administration of audit event, log and report data important to a consumer's particular information or applications.

Security compliance has a tendency to be a significant component of any compliance system. There are three critical areas where the consideration of security techniques for cloud computing are of particular interest to cloud consumers and to auditors: 1. Understanding the internal control environment of a cloud provider, including risks, controls and other administration issues when that environment touches the provision of cloud services. 2. Access to the corporate review trail, including work process and authorization, when the audit trail compasses cloud services.3. Certification of the offices for administration and control of cloud services made accessible to cloud consumers by cloud providers and how such offices are secured.

Auditing is key: The security audit of cloud service providers is a fundamental part of the security considerations for cloud consumers. Audit should be done by properly skilled staff, either having a place with the consumer or to an independent auditing organization. Security audit should be done on the basis of one of the secured measures for security controls. Consumer needs to check that the sets of controls set up meet their security necessities. There is additionally a need to guarantee proper combination of the cloud provider's reporting and logging facilities with the consumer's frameworks, so that proper operational and business information streams on a timely basis to empower consumers to deal with their utilization of provider services.

C. Manage Individuals, Roles and Identities

Consumers must guarantee that their cloud provider has procedures and functionality that governs who can access the consumer's information and applications. This guarantees access to their cloud environments is controlled and managed. Organizations manage handfuls to a large number of representatives and clients who access their cloud applications and services, each with differing roles and entitlements. Cloud providers must permit the cloud consumer to assign and deal with the roles and related levels of authorization rights for each of their clients as per their security approaches. These roles and authorization rights are connected on an every resource, service or application basis. For instance, a cloud consumer, as per its security approaches, may have a representative whose role allows them to create a buy demand, yet a different role and authorization rights is allowed to an alternate employee in charge of favoring the appeal.

The cloud provider must have a safe framework for provisioning and managing remarkable identities for their clients and services. Such Identity Management functionality must help basic resource gets to and powerful consumer application and service workflows. A key necessity for moving a consumer application to the cloud is surveying the provider's capacity to permit the consumer to assign their client identities into access groups and roles that reflect their operational and business security approaches.

Any client access or association with the provider's management platform, despite of role or entitlement, should be checked and logged to give auditing of all access to consumer information and applications. Cloud providers should have formalized methods for dealing with their own employee access to any h/w or programming used to store, transmit or execute consumer information and applications, which they should disclose and exhibit to the consumer.

D. Ensure Legitimate Security of Information and Data

Information is at the center of IT security concerns toward any organization, whatever the type of framework that is utilized. Cloud computing does not change this, yet cloud computing does bring an included focus due to the distributed nature of the cloud computing framework and the shared responsibilities that it includes. Security considerations apply both to information at rest furthermore to information in movement, both of which may require specific consideration when utilizing cloud computing services.

Basically, the questions relating to information for cloud computing are about different types of risks: risk of stealing or unauthorized disclosure of information, risk of altering or unauthorized modification of information, risk of loss or of inaccessibility of information. It is additionally worth recalling that on account of cloud computing, information resources may well incorporate things, for example, application programs or machine pictures, which can have the same risk considerations as the contents of databases or information documents.

The kind of cloud service is likely to influence the key question of who is in charge of handling specific security controls. For Iaas, more responsibilities are likely to be with the consumer; for Saas, more responsibilities are likely to be with the provider, since both stored information and the application code is not directly visible or controllable by the consumer. The key steps consumers should take to guarantee that information included in cloud computing exercises is appropriately secure: create an information resource index, consider all manifestations of information, consider privacy prerequisites, apply privacy, uprightness and accessibility and apply character and access administration.

The greater part of the security systems and technologies included are not new, in spite of the fact that cloud computing can make new considerations. For instance, if encryption is utilized on some information, how are the encryption keys managed and utilized? What's more, the path in which security is connected will doubtlessly rely on upon the way of the cloud service being offered.

E. Enforce Privacy Approaches

Privacy is gaining in significance over the globe, regularly including laws and regulations, identifying with the procurement, storage and utilization of personally identifiable information (PII). Commonly, privacy infers constraints on the utilization and accessibility of PII, with related necessities to tag the information suitably, store it safely and to allow get to just by properly authorized clients. This requires suitable controls to be set up, especially when the information is stored within a cloud provider's base. In numerous nations, various laws, regulations and different orders require public and private organizations to secure the privacy of individual information and the security of data and machine frameworks.

At the point when information is transferred to a cloud computing environment, the responsibility regarding securing and protecting the information regularly stays with the consumer, regardless of the fact that in a few circumstances, this responsibility may be shared with others. At the point when an organization depends on a third party to host or process its information, the information controller stays subject for any loss, harm, or abuse of the information. It is reasonable, and may be legitimately required, that the information controller and the cloud provider go into a composed (lawful) agreement that clearly characterizes the roles, desires of the parties, and allots between them the numerous responsibilities that are appended to the information at stake.

It is discriminating that privacy issues are satisfactorily tended to in the cloud contract and service level agreement (SLA). If not, the cloud consumer ought to consider interchange method for attaining to their objectives including looking for an alternate provider, or not putting delicate information into the cloud computing environment.

F. Ensure Cloud N/Ws and Connections are Secure

A cloud service provider must attempt to permit real n/w traffic and drop malignant n/w traffic, pretty much as some other Internet-connected association does. Still, unlike numerous different organizations, a cloud service provider won't essentially recognize what n/w traffic its consumers plan to send and get. In any case, consumers should expect certain outer n/w perimeter security measures from their cloud providers. It is suggested that consumers assess the outer system controls of a cloud provider focused around the areas: Traffic screening, Intrusion detection/avoidance, Logging and notifications.

Cloud computing incorporates various resources that are not shared in a conventional server farm. One of these resources is the cloud provider's inside n/w infrastructure, for example, the access switches and routers used to join cloud virtual machines to the provider's backbone n/w. Inner system security varies from outer n/w security; a few attackers have already made it through the outside defenses, either by means of an attack or, all the more normally, because the attackers are legally authorized for a different part of the n/w. After a client is permitted access to a portion of the cloud service provider's n/w, the provider has various extra responsibilities regarding inner n/w security. The essential classifications of interior n/w attacks that consumers should be concerned with include: Confidentiality breaches, Integrity breaches and Availability breaches.

Consumers must assess the cloud service provider's inside n/w controls as for their requirements and any current security strategies the consumer may have. Each consumer's necessities will be distinctive; however it is recommended that consumers assess the inner n/w controls of a service provider focused on the areas: Protect customers from each other and the provider's n/w, Monitor for interruption endeavors.

G. Evaluate Security Controls on Physical Framework and Facilities

An important consideration for security of any IT system concerns the security of physical framework and facilities. On account of cloud computing, these considerations apply, yet it will frequently be the situation that the framework and facilities will be possessed and controlled by the cloud service provider and it is the responsibility of the cloud consumer to get confirmation from the provider that suitable security controls are set up. Affirmation may be given by method for audit and appraisal reports.

A concise description of the security controls that should apply to the physical framework and facilities of a cloud provider involves: Physical framework and facilities should be held in secure r areas, Protection against outer and environmental threats, Control of faculty working in secure zones, Equipment security controls, Supporting utilities, for example, power supply, gas supply, and water supply should have controls set up, Control security of cabling, Proper supplies support, Control of removal of assets, Secure transfer or re-use of equipment, Human resources security, Backup, Redundancy and Continuity Plans.

H. Manage Security Terms in the Cloud SLA

Since cloud computing normally includes two associations - the service consumer and the service provider, security responsibilities of each one party must be made clear. This is commonly done by method for a service level agreement (SLA) which applies to the services provided, and the terms of the agreement between the consumer and the provider. The SLA should determine security responsibilities and should involve perspectives, for example, the reporting of security breaches. It should be expressly archived in the cloud SLA that providers must tell consumers about the event of any breach of their framework, despite of the parties or information directly affected. The provider should involve particular pertinent data in the notice, stop the information breach as fast as possible, restore secure access to the service as quickly as possible, apply best-practice forensics in researching the circumstances and reasons for the breach, and make long-term framework improvements to adjust the underlying causes of the breach to guarantee that it doesn't recur.

An information compliance report should be needed from the cloud provider and reflects the quality or shortcoming of controls, services, and mechanisms supported by the provider in all security areas. The importance of role clarity is expanded when talking about security implications. This is likewise complicated by the cloud computing technical architecture. Each one cloud computing model requires different responsibilities regarding the provider and consumer. In the Iaas model, the onus for securing and reporting upon the framework falls on the provider, yet all responsibility regarding the s/w stack from the OS to the application is the responsibility of the consumer. In the Paas model, the provider is in charge of securing the framework and platform, and the responsibility of the application lies with the consumer. At long last, in the Saas model, the provider has complete responsibility regarding security. Indeed in an occurrence where the provider bears all

responsibility, the consumer should accept that the provider has founded the proper measures to guarantee a safe domain.

5. Understand the Security Necessities of the Exit Process

The exit process or end of the utilization of a cloud service by a consumer requires careful consideration from a security viewpoint, it is vital that once the consumer has finished the end procedure, reversibility or the privilege to be overlooked is accomplished - i.e. none of the consumer's information should stay with the provider. The provider must guarantee that any duplicates of the information are wiped clean from the provider's environment, wherever they may have been stored including backup locations and online data stores. Note that other information held by the provider may need purifying of data relating to the consumer (e.g. logs and audit trails), even some jurisdictions may need retention of records of this sort for defined periods by law. Obviously, there is the opposite issue during the exit process itself - the consumer must have the capacity to guarantee a smooth move, without loss or breach of information. Consequently the exit process must permit the consumer to recover their information in a suitably secure structure, backups must be held for agreed periods before being disposed of and related event logs and reporting information should likewise be held until the exit procedure is finished.

6. Conclusions

Now days, the utilization of the cloud computing has started to spread in the world. Cloud computing is a decent opportunity for enterprises to cost investment funds and computational prerequisites. However, security and privacy risks are a significant issue for enterprise. For that reason, cloud computing consumer must investigate all cloud computing providers when they choose to take cloud computing service. The consumer achieves this by ensuring that the agreement with the provider and its connected Service Level Agreement (SLA) has fitting provisions for security and privacy. Particularly, the SLA must help keep up lawful assurances for security relating to data put away on the provider's framework. The consumer should likewise guarantee fitting mix of the cloud computing services with their own particular frameworks for overseeing security and privacy.

References

[1] Daniel J. Abadi, Data Management in the Cloud: Limitations and Opportunities, *IEEE Data Engineering Bulletin, Volume 32*, March 2009, 3-12.
[2] "The benefits and challenges of cloud computing", http://www.moorestephens.com/cloud_computing_benefits_challenges.aspx/,2013.
[3] Luis Vaquero, Luis Rodero_Merino, Juan Caceres, Et al, " A break in the clouds: towards a cloud definition ," ACM SIGCOMM Computer Communication Review, vol.39, pp. 50-55, 2009.
[4] Cloud Computing –A Practical Approach by Velte, TataMcGraw-Hill Edition(ISBN-13:978-0-07-068351-8).
[5] F. Sabahi, "cloud computing security threats and responses",International conference on communication software and Networks (ICCSN), IEEE,2011.
[6] C. Wang, Q.Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010 Proceedings IEEE, march 2010, pp. 1-9.
[7] "Service level agreement definition and contents", http://www.service-level-agreement.net, accessed on March 0,2009.
[8] "Server Intellect Service Level agreement", http://www.serverintellect.com/legal/sla.aspx, accessed on April 09, 2009.
[9] "Seccure group addresses cloud computing risks", http://www.secpoint.com/security-group-addresses-cloud-computing-risks.html, April 25, 2009.
[10] Amies, Alex; Sluiman, Harm; Tong, Qiang Guo; Liu, Guo Ning (July 2012). "Infrastructure as a Service Cloud Concepts". Developing and Hosting Applications on the Cloud. IBM Press. ISBN 978-0-13-306684-5.
[11] Boniface, M. et al. (2010), *Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds*, 5th International Conference on Internet and Web Applications and Services (ICIW), Barcelona, Spain: IEEE, pp. 155–160,doi:10.1109/ICIW.2010.91