CLOUD COMPUTING SERVICE MODELS: A COMPARATIVE STUDY

Article *in* IEEE Network · March 2016

CITATIONS
13

READS
10,130

2 authors:

Qahtan M. Shallal
Southern Technical University -Iraq
13 PUBLICATIONS **83** CITATIONS
SEE PROFILE

Mohammad Ubaidullah Bokhari
Aligarh Muslim University
58 PUBLICATIONS **516** CITATIONS
SEE PROFILE

Cloud Computing Service Models: A Comparative Study

Mohammad UbaidullahBokhari
Dept. of Computer Science,
Aligarh Muslim University
Aligarh, INDIA
Email ID: mubokhari.cs@amu.ac.in

QahtanMakkiShallal
Dept. of Computer Science,
Aligarh Muslim University
Aligarh, INDIA
Email ID: qahtan.mekki@yahoo.com

YahyaKordTamandani
Dept. of Computer Science,
Aligarh Muslim University
Aligarh, INDIA
Email ID: Yahya.kord@gmail.com

***Abstract*— cloud computing still suffer of many security issues that required the researchers to focus on it to make the users fully trust on it. In this paper we explain the security issues which attached to each service models Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS). Furthermore, a comparative study has been presented for the three service models to evaluate their performance with rang of specific factors such as characteristics, Typical level of control granted to cloud consumer, provider and consumer activities.**

Keywords- cloud computing; SaaS; PaaS; IaaS; characteristics.

I. INTRODUCTION

Cloud computing is a technology in which hardware and software resources such as special applications, CPU, Storage and many other are provided to users as a service in basis of pay as you use and through the internet, these resources has the ability of automatic scaled up and down according to the client's demand. The cloud computing technology has many features such as pay as you use, high scalable, easy to access, lowering business risks and maintenance expenses, reducing operating cost [1][2]. In 1960 John McCarthy guest in the future the computing facilities will be deliver as a service to clients such as utility (electricity, water, gas) [3]. In 1990 the ''cloud'' has been presented in form of ATM networks. In 2006, Eric Schmidt who is Google's CEO providing service via internet by the use the word to depict the business model. So from 2006, cloud computing became famous and interested to marketing terms to represent a lot of various ideas [4]. This study deeply explain the three type of service models in cloud computing which are Software as a service SaaS, Platform as a service PaaS and Infrastructure as a service IaaS.

II. CLOUD COMPUTING SERVICE MODELS

There are three models of service in cloud which are software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS), figure (1.1) is explain the three service models.

B. Software as a service (SaaS)

1) Review of SaaS technology:

It is a model which allow the clients to use and rent the applications from the provider without install it on their own PC [5]. This is mean the licensed applications which been provided to clients are running on cloud's infrastructure through the interface of thin/thick client such as Google chrome, internet explorer and many others. Software-as-a-service is a service where the actual development of software and applications takes place on the platforms provided by the PAAS layer. SaaS layer is mainly concerned with end users because end users can access and use these applications which were made by cloud providers [6] [7]. The management and control of the infrastructure will be under the provider responsibility, only limit number of customers would have their own configurations [8] [9], the set of predefine configuration options will be used to customize the applications [10] [5]. SaaS model is classified as a best way to get the light weight applications such as Microsoft word, Microsoft access, media player and so on. The problem here is the slow of network is causing dead the time of processing the data for heavy weight applications such as 3D games [8]. The cost of SaaS applications is different from one application to another, some providers charge the client a flat rate irrespective of the usage, whereas the other is charging the client according to usage [11].

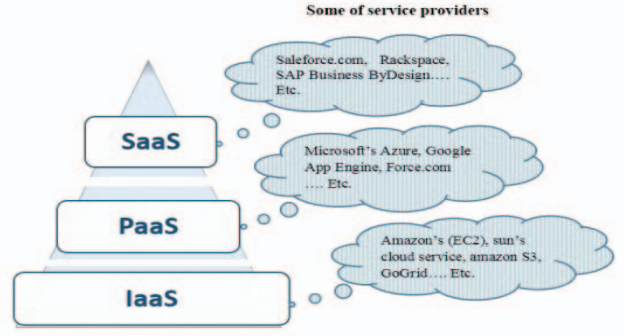

Fig. 1. Cloud-computing: the three layers of generic model

C. Advantages of SaaS technology:

There are many advantages of using SaaS model such as [11][12][13]:

- Reduce the application software licensing cost.
- SaaS is handover the application to clients in basis of one-to-many, so one application could be run by many

clients in same time.
- The applications provider will be responsible to control and limit the use of applications.
- It remove the need of infrastructure. Because it is use the infrastructure of cloud itself.
- The applications of SaaS model can be configure by API, but it cannot be fully customize.
- Secure socket layer (SSL) used in SaaS model.

D. Security of SaaS technology:

For appropriate security, the client in SaaS model is relying on the provider of service. The security challenges of SaaS are mostly similar to the security challenges of web application [14]. The security issues in SaaS model is explained as below:

1) Security of the data: To retrieve or store data in cloud, user need to transmit them through internet. Thus an effective techniques of encryption must be applied to data for secure them and some other techniques must be used to ensure the authorization and authentication for control the access to data [15][16].

2) Locality of the data: When the service provider get our data, immediately will distribute many copies of them into many cloud data centers which located in different countries, so the client does not aware where his data is locate. Moreover, each country has its legislations to data. Hence, the client is not able to recognize which legislations will be applied to his data. This issue is still unclear in cloud computing [17][16].

3) Data Privacy: Privacy is refer to prohibit the unauthorized user to access the sensitive data. Cloud computing is allowing the data of different users to be shred in same infrastructure, these data could be belongs to multimedia, health records, small organization, big organization and many more. So, the privacy question will be appear when the data got accessed by other users. This will lead to privacy issues. Dropping the privacy results to data leakage. To accomplish the privacy, strong data encryption, giving user ID and password for each user, biometric verification, key fobs/soft tokens, two-factor authentication, One Time Password and security tokens must be considered [16].

4) Integrity of the data: It means that the data should be same as it is during entire cycle of life. Only the authorized user is able to change his own data. So, it must not changeable by unauthorized user during the transmission or in provider's data centers. The main threats to data integrity are manipulation and data loss and malicious computation. The integrity of data can be accomplished by executing Meta data and check sums of the files. Redundancies or backups must be apply to restore the data which been effected to its original state [16].

5) Data isolation: The infrastructures of cloud such as storage, servers and so on are shared by many organizations, which is put the particular data of organization in risk. Thus, the user will be having doubt on the ability of provider to apply a proper isolation of his data from the other users [16].

6) Accessibility of data: Cloud requires a proper control for central access of user where every user need to use any service provider is restricted by the entitlement information and identity of user. The identity is linked to the domain, but is not fixed due to the possibility of changing employees at any time or changing their positions. The approach of user centric gives the user a maximum control over their digital identities [16][18].

7) Sniffing of data on the Network: Cloud will process the sensitive information of client by SaaS application and then store processed information in SaaS vendor. The clients must transfer their data over the network. Hence, these information need to protect from network attackers. So the security weakness of networks will lead the malicious to sniff the packets of data. There is possibilityof hijack the active sessions. This needs strong techniques of encoding such as TLS and SSL to secure the data over the network [16][19].

8) Authentication, authorization and identity management: The authentication and identity management are very important in cloud computing. The process of verify the identification of eligible users and protecting these credentials are issue part of authorization and authentication in cloud. Service hijacking and account involves manipulation the vulnerabilities of software and data where attackers acquire credentials and unauthorized access has obtain to data centers and application servers [20][16]. Such type of unauthorized access is having impact on the issues of availability, confidentiality and integrity of services and data. Furthermore, the harmful insiders which include dishonest administrators will affect hardly on the security of organizations. The present mechanisms of authentication probably are not useful in the environments of cloud as the customers no longer would be able to get access a single controlled system or belong to. Also the unauthorized access may occurred through the vulnerabilities of web browser. By using a constraints on the IDs of user the management of identity is responsible to identify the individual users uniquely and handling their own accessibilities. The problems will possibly appear because of the replicated IDs, this need to be managed to secure the data of user [16].

9) Web application security: Attacks are targeting the services, software and applications which are commonly in web. Both SaaS and web applications are providing a good service to end users. By using automated tools the threats can attacks the web applications. Usually attackers are use the web to steal the sensitive data of particular computer. The major threats for web applications which been documented by Open Web Application Security Project (OWASP) are: SQL injection, Cross-Site Scripting hits, Denial of Service, Buffer Overflows anomalies, Session Hijacking and Insufficient transport layer security [16][21].

10) Vulnerability in virtualization: Virtualization is used to fully utilize the resources of IT such as network, processor and storage to avail and reduce the IT resources cost. The existing Virtual Machine Monitor (VMM) does not support a perfect separation for the physical machines. The most popular threats in virtualization are: Virtualization Capacity Planning, Virtual Machine Threat,Vm Sprawl, Hypervisor Threat, Virtual Infrastructure, Virtual Network Threat, Virtualization Backup And Recovery, and Vm Stall [22][16].

11) Availability: SaaS must ensure the services are available to users 24/7. By doing a proper and continuous maintenance for both software and hardware resources, the availability will be guaranteed. Also its substantial to keep the current along with all necessary improvements of system, giving good enough bandwidth of communication and avoiding the blockage appearance are extremely important. When the issues of hardware occurred the network intrusions, RAID, attacks of denial-of-service, failover and redundancy can result to major consequences. Quick recovery for the disaster is primary. For connections disruption or data loss the protection must apply, even for the actions which are unexpected which can include fire and natural disaster. To prevent the loss of data from these occurrences, copies of backup must be distribute to many other locations to be saved as well as waterproof and fireproof safe [16][23].

12) Backup: There are some drawbacks when we use the provider of cloud backup which can included as following [16]:

- The issues of latency: especially when willing to back-up a large size of data.
- Safeguard the data by handover it to the third parties: when the data is not encrypted so they need to do encrypt backups before send to them.
- Users generally are relying on the backup of cloud provider, are users aware of what happened if the provider stop giving the services to them.

D. Platform as a service (PaaS)

D.1. Review of PaaS technology:

It is provide a proper environment or platform in which the developer can develop the applications and software to deploy them through the internet without any need for install or manage the development environment [10][24]. PaaS is allowing the customer to rent virtualized servers and attached services for execute available applications or develop and test the new one [25]. The customer does not control over the cloud's infrastructure such as servers, networks, storage or OS, whereas the customer has the control over the deployed applications and their configurations [8]. The cost of service will be determined according to: data transfer per GB, usage per hour, I/O requests per million, storage use per GB and datastorage requests per thousand [2].

D.2. Advantages of PaaS technology:

There are many advantages of using PaaS models such as [25][12][13]:

- Increase the flexibility for the development process and decrease the server storage overhead.
- Streamlined version deployment.
- The security is provided, containing data security, recovery and backup.
- Reduce the cost by rent the physical and removing the need of expert people to manage the infrastructure.
- Adaptability, that mean it has the ability to change if the circumstances are altered.
- PaaS is working on basis of one-to-many, so many developers can work on same application.
- Flexibility: customers are able to control on the tools which are installed along with their platforms, and have the ability of create new platform to fit on their special requirements.

D.3. Security of PaaS technology:

The security issue in PaaS is a big concern and will be distributed to the responsibility of both developer and provider, the developer will be responsible to secure his applications themselves, whereas the provider is responsible to secure the development environment and computing platform [26][14]. There are many security issues associated to PaaS model such as:

1) Third-party relationships and web hosted development tools: PaaS is serving third party web services Mashups to clients. Mashups is web application or pages which combines the necessary elements from more than one resources to be a single unit [27][16]. Hence, the model of PaaS will be having same security issues which belong to Mashups such as network and data security [16].

2) Lock In of PAAS Vendor: The vendors of PaaS are able to control over the application framework and storage which used by applications, what eventually occurs towards the organizations which need from the infrastructure to operate their apps [16].

3) Rapid change of application: The developers are facing difficulty for construct a secure applications which are going to be hosted in cloud. The quick change of application in cloud will impact on System Development Life Cycle (SDLC) and security [28][16]. The developers must be aware of continuously doing upgrade to their applicationin order to keep the changes for their applications. Also, the developers must be aware of the legal issues of data which will be stored in different locations and different rules [16].

4) Disaster and business stability arrangement: There are many doubts in this issues which are related to platform of cloud computing. Developers does not know what will happens if the service shutdown due to many reasons. Also they do not know who will be responsible to fix the problem. Moreover, the organization does not know how this outage will impact on the ability of organization to conduct its business [16].

5) Security of underlying infrastructure: The developers in PaaS model cannot access to the cloud's core layers. Thus, the responsibility of cloud service provider is to secure the application services and underlying infrastructure. SaaS applications are created by the help of development tools which provided by PaaS model. The developers are not pretty sure regarding the development tools security which been provided by provider of PaaS, despite the developers are having control on their applications [16] [29].

E. Infrastructure as A Service (IaaS)

E.1. Review of IaaS technology:

It is provide the virtual infrastructure and raw hardware which can be create, manage and destroy storage, and VMs via web based service [7][24]. IaaS model is a result for the evolution of virtual private server which been already known since many years back [9]. The provider of IaaS is supplying the client with virtual server along with one or more CPU executing several choice of operating [5][10]. The VM might be rent either for an hour or it could be rented as long as it need. The infrastructure resources are able to scale up and down according to client's demand and will be billed depend on the amount, duration, and additional services which been used by client form the VM. Some providers are allowing the virtual instances to be connected to the company's network through virtual private network (VPN) to make the network of the company appear as a one big scalable IT infrastructure [9]. The provider is responsible for operate, hosting and maintain the infrastructure in order to serve the client [24][25]. The client is able to control over the IP address, CPU, Memory, storage, deployed applications, OS and some limit number of selected components of the networking. The cost of use is predominantly similar to the structure of PaaS [2][24][25].

E.2. Advantages of IaaS technology:

There are many advantages of using IaaS models such as [25][12][13]:

- The client able to increase or decrease the infrastructure on demand.
- The client able to execute a virtual machine due to providing virtualization as a service.
- Network as a service are provided, which includes the load balancing, hardware for routers and firewalls.
- Reducing the cost of human resources and hardware.
- Reducing ROI risk and low obstacles to entry.
- Automated scaling and streamlined.

E.3. Security of IaaS technology:

The developer in IaaS model have much control on the security as well as there are no holes of security in virtualization manager [30][14]. As an addition, in theory the virtual machines may possibly be able to direct those type of issues but also in practice you can still find several problems of security. Another factor would be the data reliability which have stored inside the hardware of provider. As a result of getting larger virtualization of 'everything' in the society of information, keeping the maximum control on data to the data owner irrespective of the physical location of it will come to be a topic of the most interest. In order to accomplish maximum level of security and trust on the resource of cloud, many different techniques should be applied [31][14]. The client is responsible for controlling the security that relevant to IT system including the data, applications and operating system [14]. There are many security threats to IaaS, we are going to mention some of them as below:

1) Attacks in Virtualization: By the help of virtualization the users can use the physical resources to create new layer such as network resources, storage device, server or OS to operate their applications. As the virtualization have advantages, it is also have disadvantages by allowing the attacker to gain access to physical machine [32][16]. by considering all attacks type, the Virtualized environments are weaker than normal infrastructures. Furthermore, two boundaries will be for VMs, which are virtual and physical. Also virtual machine of malicious can be migrated to another host to compromise it [16].

2) Weak SLAs: SLA will assures the QOS acceptance level from the provider to customers, the SLA explains the definition of contract, monitoring, enhancement and negotiation of resources [33][16]. Negotiation and contract definition is important to have knowledge on the responsibilities and benefits for every party. The absence of standardization in the cloud-based services will cause to absence of clarity in SLA agreements which offered by various providers, it certainly will impact on the security as well as expose the client to many vulnerabilities [16].

3) Shared resources Vulnerability: One server is able to share many resources such as I/O, memory, CPU and many other resources to various VMs based on it. These shared resources might lead to breach for other VM [16]. The malicious VM may decide to go over communication with the other VMs via shared memory. By using hidden channels, any two of VMs can be communicated by pass a way of all the laws which defined by the VMM security module [34][16]. The malicious Virtual Machine is able to monitor the resources which are shared without really being pointed out through the act of its VMM, due to this hole the attacker can gain the information of other VMs [16].

4) Life cycle of Virtual machine: There is possibility of VMs to be suspended, off or on by the code of malicious [16]. It is very difficult to detect the malware, they can threat the VMs even if they were offline because the virtual machine could possibly be instantiated by using an image which could have a malicious code [35][16]. These malicious code and images can possibly be injected with the other VMs in the process of creation [16].

*5) Data Loss and Leakage:*Many individual users can share the data by using IaaS in public cloud. Particular user is not sure who, how and from where attacker will gain access to his data. These issues can be avoided or reduced by applying a strong techniques to protecting the data, authorization and authentication [16].

III. COMPARATIVE STUDY

We make a comparative study between the three models of service SaaS, PaaS and IaaS according to theoretical papers base on many factors as we listed in the table below [5][7][25][36].

TABLE I. COMPARISON TABLE AMONG THE THREE MODELS OF SERVICES SAAS, PAAS AND IAAS

Model / Factors	SaaS model	PaaS model	IaaS model
Characteristics	• Users are provided with applications that are accessible anytime and from anywhere, these applications are provided in one-to-many mechanism. • Access via web to commercial software. • User does not need to manage the software such as upgrade and patches. • Application Programming Interfaces is giving the ability the different pieces of software to be integrated • SLAs. • UI powered by "thin client" applications. • Stateless and loosely coupled. • Modular. • Semantic interoperability. • Centralized Hosting / Delivery. • Uniform Platform for Delivery. • Open Collaboration / Sharing.	• Users are provided with a platform for developing applications hosted in the Cloud. • Services to develop Test Deploy host and maintain applications in the same development environment. • Web based user interface creation tools help to modify, create, deploy and test different UI scenarios. • Same development application could be utilize by many users. • Web service and database are integrated with PaaS via common standards. • Support for development team collaboration. • Tools available to handle billing and subscription management. • User interface is Customizable /Programmable. • Database Customizations are unlimited. • Solid Workflow engine/capabilities. • Flexible "services-enabled" integration model. • It is consumes cloud infrastructure;	• Users are provided with virtualized hardware and storage on top of which they can build their infrastructure • Allows for dynamic/self scaling. • It has alterable cost, utility pricing model. • Ability to provide single hardware to many users. • Supported OS and Platform independent. • The costs are less due to the share of infrastructure. • (SLA) Service level agreements. • Pay as you go. • Applications/frameworks.
Typical level of control granted to cloud consumer	Usage and usage-related configuration	Limited administrative	Full administrative
Consumer activities	User and configures cloud service	Test, develop, manage and deploy cloud based solutions and cloud services	Configure and setup bare infrastructure, install, manage and monitor any required software
Provider activities	Manage, maintain and implement cloud service monitor usage by consumer of cloud	Pre-configure platform and provision underlying infrastructure, middleware and other required IT resources as requisite monitor usage by consumer of cloud	Manage and provision the storage, physical processing, hosting and networking the required monitor usage by the consumer of cloud
Services	Email, CRM, website testing, Virtual desktop, Wiki, Blog, automation	Service and application test, development, integration and deployment	Virtual machine, operating system, message queue, network, storage, CPU, memory, backup service
Vendors	Saleforce.com, Google documents, Clarizen.com, project management, Facebook.com, Gmail, Hotmail, Quicken online, Netsuite, , IBM®	Google AppEngine, Microsoft Azure, Yahoo developer Network, MSFT, Heroku, Engine Yard, force.com	Amazon EC2 and S3, Gogrid, RACKSPACE, IBM BlueHouse, Linode, VMWare

IV. CONCLUSION

In this paper we examined the three service models of cloud computing (SaaS, PaaS, IaaS). The paper has focused on the security issues of each model, advantages associated to them and comparative study has been done among them. This comparative study assisted the clients of cloud to determine what the kind of service's characteristics they need, as well as the risks type which attached to each model. In spite of there are many advantages attached to each model also there are many security, SLA and privacy issues attached to each model which are scare the users to shift his own work to cloud computing. Moreover, cloud computing is located in a specific location which users does not know where it is, the user is send/receive the data through the internet and the users use same infrastructure to store and process their data. Then integrated solution should be suitable for every vulnerabilities to make users having faith on the technology. Furthermore, there are security issues attached to network connection between user and cloud computing, the network attacker can get, snoop or alter data during transmission.

REFERENCES

[1]. Kesan, J. P., Hayes, C. M., & Bashir, M. N. Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency. Wash. & Lee L. Rev., 70, 341. 2013.

[2]. Z. Mahmood, "Cloud Computing: Characteristics and deployment approaches," Proc. - 11th IEEE Int. Conf. Comput. Inf. Technol. CIT, pp. 121–126, 2011.

[3]. Buyya, Rajkumar, Christian Vecchiola, and S. ThamaraiSelvi. Mastering cloud computing: foundations and applications programming. Newnes, 2013.

[4]. Weinhardt, Christof, et al. "Cloud computing–a classification, business models, and research directions." Business & Information Systems Engineering 1.5 (2009): 391-399.

[5]. D. Rani and M. T. C. S. E. Student, "A Comparative Study of SaaS , PaaS and IaaS in Cloud Computing," vol. 4, no. 6, pp. 458–461, 2014.

[6]. ON, T. F. Cyber Security and Reliability in a Digital Cloud. 2013.

[7]. A. M. MayankaKatyal, "A Comparative Study of Load Balancing Algorithms in Cloud Computing Environment," Int. J. Distrib. Cloud Comput., vol. 1, no. 2, p. 14, 2013.

[8]. O. P. Karada, A. Pipliya, P. Thakur, and N. Kamdar, "Analytical Survey Model on Consumption of Cloud Service Models," pp. 46–50, 2011.

[9]. C. N. Höfer and G. Karagiannis, "Cloud computing services: Taxonomy and comparison," J. Internet Serv. Appl., vol. 2, no. 2, pp. 81–94, 2011.

[10]. [10] Kavis, M. J. Architecting the cloud: Design decisions for cloud computing service models (SaaS, PaaS, AND IaaS). John Wiley & Sons. 2014.

[11]. G. Kulkarni, P. Chavan, H. Bankar, K. Koli, and V. Waykule, "A New Approach to Software as Service Cloud," 2012 7th Int. Conf. Telecommun. Syst. Serv. Appl., pp. 196–199, 2012.

[12]. L. Tim Mather, SubraKumaraswamy, "Cloud Privacy and Security," Gov. An Int. J. Policy Adm., p. 336, 2009.

[13]. M. Computing, D. Thakral, and M. Singh, "Virtualization in cloud computing 1," vol. 3, no. 5, pp. 1262–1273, 2014.

[14]. R. Article, "SECURITY CHALLENGES IN DIFFERENT DELIVERY MODEL SPECIFICALLY SaaS," 2015.

[15]. Yu, Shucheng, Wenjing Lou, and KuiRen. "Data Security in Cloud." Handbook on Securing Cyber-Physical Critical Infrastructure (2012): 389.

[16]. G. Kalpana, P. V Kumar, and R. V Krishnaiah, "A brief Survey on Security Issues in Cloud and its service models," vol. 4, no. 6, pp. 457–463, 2015.

[17]. Birk, Dominik, and Christoph Wegener. "Technical issues of forensic investigations in cloud computing environments." Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on. IEEE, 2011.

[18]. Pinnaka, Chaitanya. "Quantification of User Privacy Loss." (2012).

[19]. InamulHaq, Muhammad. "The major security challenges to cloud computing." (2013).

[20]. Bhadoria, Robin Singh. "Security Architecture for Cloud Computing." Handbook of Research on Securing Cloud-Based Databases with Biometric Applications(2014): 47.

[21]. Brooks, Tyson, et al. "Secure the edge? Understanding the risk towards wireless grids Edgeware technology." International Journal of Internet Technology and Secured Transactions 8 5.3 (2014): 191-222.

[22]. Shi, Weidong, et al. "Architectural support of multiple hypervisors over single platform for enhancing cloud computing security." Proceedings of the 9th conference on Computing Frontiers. ACM, 2012.

[23]. denUijl, Maarten, JorisHulstijn, and Fred van Ipenburg. "An integrated platform for supply chain transparency: a case in the cocoa industry." (2013).

[24]. J. Gibson, R. Rondeau, D. Eveleigh, and T. Qing, "Benefits and challenges of three cloud computing service models," Comput. Asp. Soc. Networks, pp. 198–205, 2012.

[25]. S. Khurana and A. G. Verma, "Comparison of Cloud Computing Service Models : SaaS ,PaaS , IaaS," Int. J. Electron. Commun. Technol., vol. 7109, pp. 29–32, 2013.

[26]. Bacon, Jean, et al. "Information flow control for secure cloud computing."Network and Service Management, IEEE Transactions on 11.1 (2014): 76-89.

[27]. Marston, Sean, et al. "Cloud computing—The business perspective." Decision Support Systems 51.1 (2011): 176-189.

[28]. Markov, Georgi A. Towards an industrial ALM (Application Lifecycle) Tool Integration. Diss. Blekinge Institute of Technology, 2011.

[29]. Marston, Sean, et al. "Cloud computing—The business perspective." Decision Support Systems 51.1 (2011): 176-189.

[30]. Subashini, Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.

[31]. Felter, Wes, et al. "An updated performance comparison of virtual machines and linux containers." technology 28 (2014): 32.

[32]. Moreno-Vozmediano, Rafael, Rubén S. Montero, and Ignacio M. Llorente. "IaaS cloud architecture: From virtualized datacenters to federated cloud infrastructures." Computer 12 (2012): 65-72.

[33]. B. Kepes, "Understanding the Cloud Computing Stack SaaS, Paas, IaaS," pp. 1–20, 2013.

[34]. Futral, William, and James Greene. Intel® Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters. Apress, 2013.

[35]. Fernandez, Eduardo B., Raul Monge, and Keiko Hashizume. "Building a security reference architecture for cloud systems." Requirements Engineering(2015): 1-25.

[36]. Erl, T., Puttini, R., &Mahmood, Z. Cloud Computing: Concepts, Technology, & Architecture. Pearson Education. , 2013.