

# Cloud Computing: Issues Regarding Technology and Proposed Solutions

Sidra Sultan

Electrical Department

Institute Of Space Technology, Islamabad

[Sultan\\_sidrah@yahoo.com](mailto:Sultan_sidrah@yahoo.com)

**Abstract**— Cloud computing provides an environment where IT services and resources are made available on demand via internet. It holds the capacity of reducing cost for setting up the computing infrastructure as it is the headache of the service provider. Consumers can access cloud services at anytime, anywhere through remote data centers deployed by service providers. Cloud computing motivates organizations and individuals by its silver linings including mobility, high scalability, flexibility, multi-tenancy, shared resource pooling, reduced hardware, low maintenance, quick support and utility-based pricing. Despite, there are also thunder clouds such as internet reliability, dependence on supplier, data integrity, data theft, data loss, and privacy and security concerns. These unresolved issues have become a serious threat in the wide adoption of cloud computing. . In this paper detailed analysis of cloud computing and its pros and cons has been carried out. There is a huge room for research and development in this field as the future of computing lies in virtualization of internet services through work load shifting. Our work will enable researchers to get insight of cloud computing and help them to carry out further research regarding this topic

**Keywords**— cloud computing, virtualization, SaaS, PaaS, IaaS, challenges in cloud computing, cloud computing analysis

## I. INTRODUCTION

Due to its advancements in IT services, cloud computing is viewed as the next generation of computing. Large amount of time and energy was spent by information technology on the installation, proper maintenance and timely up gradation of set-up that are often not very significant to the company's main goal. Now by the virtue of cloud computing technology, less time is spent on un-necessary and redundant activities and the organization can focus on activities which have greater effect on business [1]. In cloud computing, the conventional vendor is comprised of two portions: the *infrastructure providers* who take care of platforms offered by cloud computing and offer resources according to a pay-as-you-use system and *service providers*, who buy resources from infrastructure providers to assist customers [2].

The paper follows the following sequence: Section III provides a comprehensive literature review of the topic. In Section IV, benefits and drawbacks of cloud computing are discussed. Section V gives recommendations for future research in this area and finally Section VI concludes the paper.

## II. OVERVIEW OF THE ARCHITECTURE

### A. Service Models

Cloud Computing consists of some reference models which forms the basis of cloud computing, these are known as service models. These models consist of three layers which are formed depending on the types of services being provided by vendor. Following three categories can be defined as the reference models of cloud computing as shown in figure 1.

### B. Software as a Service (SaaS):

SaaS resembles to the old lean client-model of software delivery in which clients with the help of web browser application access the software program being run in servers located at a remote location [3]. Servers which are service providers host the application and consumers can access them from anywhere over the internet, so it is a form of software distribution [9].

Most of the users are familiar with the service of SaaS. Some of familiar applications include Google Apps, Yahoo, App box etc. SaaS does the work of load shift from consumers to vendors and thus consumers get rid of the management of software. Users only have to pay some amount of money on monthly basis and in return get the service. It permits certain organizations for their business management at less cost. SaaS is economical because users don't have to pay for the hardware, instead SaaS do it for their customers and let them free from installation, maintenance and up gradation of software. SaaS based applications are designed in such a way that they can handle several concurrent consumers at the same time. As applications are accessed through internet via browsers, so security is one the major concern here. It is basically required to secure SaaS based applications by deploying encryption and cryptographic techniques. Some of the methods include Web services (WS) security and Secure Socket Layer (SSL) for securing the data [30].

### C. Platform as a Service:

PaaS is at the layer lower than SaaS, it consists of development tools which are hosted by service provider. Users are given the access to platform where they can do their own coding and develop their own software quickly and efficiently and put them on the cloud [3]. Multi clients make use of PaaS where they are provided with the

environment to develop codes and execute applications for their projects development [31]. Its benefit is that the need for buying special equipment, hardware and software for the development of applications is diminished [3]. Examples are Microsoft Windows Azure, Heroku, Google Apps, etc.

PaaS is highly useful in the case where there are many developers who are taking part in project development, they make use of PaaS as it provides them the platform for the deployment of their applications. Protection of data in storage is extremely important where storage is provided as a service. Therefore, integrity of data should be maintained and well defined encryption and cryptographic techniques should be applied.

#### D. Infrastructure as a Service

IaaS forms the lowest layer and is comprised of resources for the delivery of hardware services mainly using technology of virtualization. Companies make use of IaaS by giving payment on demand basis, instead of purchasing, installing and maintaining the hardware for their data centers. IaaS providers deliver their clients, the cloud servers and storage on demand via application protocol interface. IaaS users can directly access the storage and hardware provided by IaaS providers [3].

#### E. Deployment Models

Based upon the users' demands, following are the three ways of getting access to cloud:

##### a) Public Cloud

It consists of infrastructure which provides the services and applications via web applications to the general public. Services are made accessible to everyone. So there comes the concern of security and privacy of data and service being provided. Example is Email we use.

##### b) Private Cloud

It consists of infrastructure owned by the organization which provides the services which are accessible only to specific users. As, it is available only to some specific customers and is handled by the users within the organization. So, it has security and privacy of data as compared to public cloud.

##### c) Hybrid Cloud

It is deployed as per demand of organization as some of the organizations has the requirement to different types of cloud to meet user level needs.

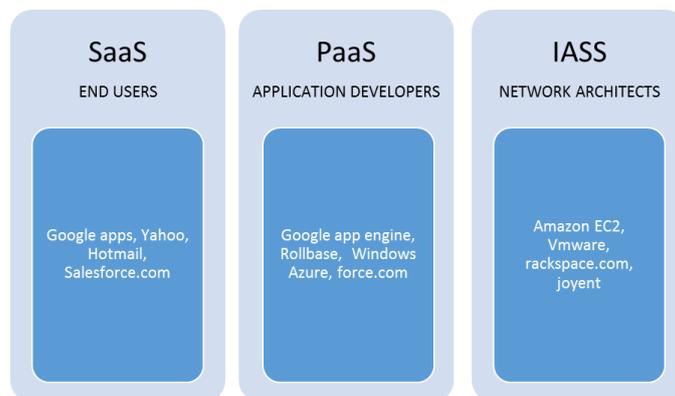


Figure 1: Cloud Computing Architecture; SaaS, PaaS, IaaS

### III. RELATED WORK

Many researches have been carried out so far in this regard. S. Zhang *et al.* [1] analyzed different aspects of cloud computing and found that security concerns are a hidden danger for cloud computing. However they believed that the technology will be irresistible, once this field found the safety control solution. K. R. Islam *et al.* [3] studied architecture of cloud computing in detail and put light on the challenges faced by it. They predicted that this technology will bring us infinite capability of computing by solving the existing issues. R. Piplode [4] discussed security issues with a focus on attacks and hacking attempts related to cloud computing vendors and systems. He anticipated the classes of security issues that would arise from cloud computing and proposed some preliminary solutions including Digital signature technique, SSL protocol, tested encryption algorithm etc. M. Z. Meetei [5] employed a simulation technique for security risks in cloud computing using Poisson process. He claimed that the simulation technique helped to enhance the accuracy in predicting high risk threats to cloud security and aimed at adopting stochastic techniques for more advanced simulations.

Wayne [6] identified main problems suspected to cloud computing security and privacy concerns. He mainly emphasized on public clouds that needs significant consideration and presented required details to assist organizations in making decisions about data security. The strong point of his effort is broad discussion on security issues in cloud computing which educates customers regarding privacy and security threats coupled with cloud services. The weak point is that he has not proposed any method or solution to deal with the identified problems.

R. D. Pietro [7] proposed a new methodology, Transparent Cloud Protection System (TCPS) for the improvement of security issues in cloud services. He claimed that TCPS can monitor cloud components integrity and ensures transparency and virtualization. His strength is his proposed tool which improves the security and transparency, and suggests mechanism to detect intrusion. The drawback is that, nor has he proved his work neither implemented it in a real cloud

computing environment. K. Munir [8] presented a physical security architecture for cloud computing. He said that the presented design can be adapted with the progress in security technologies used for its implementation. F. Bashir [9] studied security threats in cloud computing and discussed the positive and negative aspects of various researches carried out in this regard. C. Gong *et al.*[10] summarized the general characteristics of cloud computing to help user understand the basic concept and assist him in making choice among different available cloud services.

S. Zhang *et al.* [11] studied the industrial world’s 3 concrete cloud computing examples: the cloud computing platform of Google, the Amazon Elastic computation cloud and “blue cloud” of IBM and analyzed and compared the three kinds of platforms. Balachandra *et al.* [12] in their paper identified some of the service level agreements known as SLA, its specifications and goals regarding location of data, its isolation and its proper recovery. Kresimir *et al* [13] wrote about security issue in cloud computing which includes integrity of data, privacy of critical information. Jiafeng *et al.* [14] gave some background knowledge of cloud computing and discussed the service models of cloud computing. He also provided some of the current problems being faced by users including privacy of data and its security, and proposed solutions for preventing these issues. Yashpalsinh and Kirit [15] discussed the architectural design of cloud computing, its applications and pros. and cons including privacy and security as one of the main concern. Akhil and Kanika [16] provided in the paper, their research regarding challenges being faced by cloud environment because of its dynamic nature. They discussed some key solutions which can be implemented for the security of cloud service. Morsy *et al.* [17] discussed cloud architecture and showed the problems of cloud computing and wrote about the delivery models of cloud computing.

Hanim Eken [18] pointed out the risk involvement in cloud environment. He wrote about threats in security of cloud services. Those threats are mainly linked to integrity of data, the security of information and its privacy. Author has provided some recommendations regarding security of cloud service. Author has not wrote about some new innovation in cloud computing, rather its focus was on previous issues regarding security. Maneesha *et al.* [19] carried out in his paper, extensive discussion on types of clouds and their security challenges and explained how to prevent different security problems including DOS attacks and attack on VMs. The researcher has compared different service providers on different cloud services SaaS, PaaS, IaaS. Y.Chenet *et al.* [20] presented their views regarding cloud. Those views are related to multi-users concern regarding trust consideration and the required need for their mutual inspection for business accounts. They have also provided the users with some areas which need more attention as compared to others like providing isolations to multiple users. Shuai Zhang *et al.*[21] provided the comparison between cloud and Grid computing. In their view, cloud computing cannot be replaced by grids but

however the chances are that grids will be merged into cloud computing in future.

#### IV. POINTS OF ARGUMENT

##### A. Reason to Support

Cloud computing has the potential to attract customers using orthodox computing techniques with several new features:

##### B. Mobility

Since the services are web-based, now customers can access them from anywhere in the world. This enables employees to serve their company whilst on the move [4].

##### C. Scalability

It provides a service model where utilities can be leased and released by users through the internet in an on demand fashion [4].

##### D. Flexibility

Cloud computing services do not have high initial investment, therefore, customers have to pay less if they switch suppliers [23].

##### E. Multi-tenancy

Multi-tenants share the same physical and logical access to storage, database, computing, memory and other such sources in cloud paradigm [22].

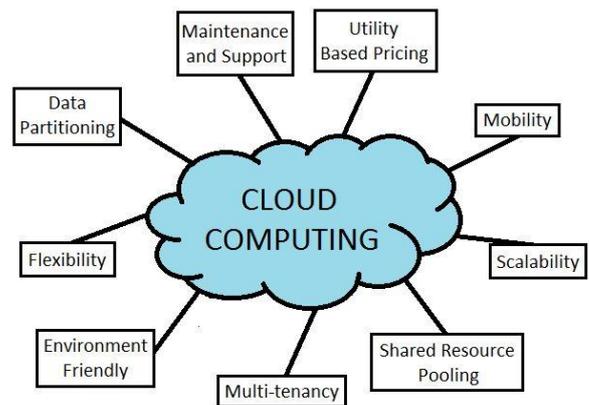


Figure. 2. Advantages of Cloud Computing.

##### F. Shared Resource Pooling

It is the sharing of computing abilities. This means you have to spend lesser and can enjoy more resources [22].

##### G. Data Partitioning

Storage of data from different tenants at different locations decreases latency and improves performance [22].

#### H. Maintenance and Support

Support services are usually offered by the supplier. However, in cloud computing, since the services are remotely hosted, therefore, maintaining and supporting processes are less interfering for the customers. Customers can piggy-back on their supplier regarding upgradation in computing resources [24].

#### I. Environment Friendly

Data centers are a 'green' alternative to in-house computing. Running capacity of a server in large data centers is higher than an in-house server. While they use slightly more energy per hour in comparison with an in-house server [25].

#### J. Utility Based Pricing

Cloud service providers introduced several models for payment. These include per month, per year, per user etc. Customers can choose the model that is best suitable for them [1].

#### K. Reasons to Oppose

The hurdles in the way of cloud computing, that do not allow its wide adoption are:

#### L. Dependency upon Vendor

Customers can only use those services which are offered by the vendor. Without the provider, user cannot get access to its data. Also, switching from one service provider to another is cumbersome as consumer has to transfer large amount of data [26].

#### M. Tenant Isolation

Different users put their data in the cloud thus forming huge data centers of cloud. It makes difficult for cloud provider to manage segregation of different data between different users [22].

#### N. System Malfunctioning

A bug can occur in the software of cloud service provider; it can cause corruption and modification of data of users. Hence, software applications are prone to attack by malicious activities and cause whole system destruction [27].

#### O. Dependency upon the Internet

Since, the cloud based application is hosted remotely, an internet connection is required to transfer user data. This makes usage of the application highly internet dependent. [28].

#### P. Denial of Service (DoS) Attack

A method that hackers deploy to crash servers are DoS attacks. In this method, the attacker sends a lot of requests to server that server cannot cope up with, hence causing the break-down of server. This is used by hackers to stop

the services of some particular web application. It has become a very serious threat in the deployment of cloud computing [29].

#### Q. Man in the Middle (MITM) Attack

This problem is caused when the sockets are not properly encrypted. Whenever a user wants to send request or receives data from server, it opens up a socket for the communication. But, the data can be leaked if the secure socket layer is not properly configured to prevent the attack and therefore causing the other person to actually track the data flowing between the user and the server [30].

#### R. Network Sniffing

Another threat to cloud computing is the improper and simple encryption techniques which can easily assist hackers to hijack sensitive information by simply hacking the passwords of the encrypted data [29].

#### S. Cross Site Scripting

In this attack, the hackers employ intelligence redirection, whenever a user enters the URL of website he wants to access. Hence, causing the user to lose its sensitive data [29].

#### T. Port Scanning

There are some ports which are always open, e.g., port 80 – Hyper Text Transfer Protocol (HTTP) for accessing the internet. Whenever, an attacker attacks, it makes use of open ports at server, thus making it vulnerable to hack [29].

#### U. Incomplete Data Deletion

Sometimes, a user requests to delete its data from the servers. Since, replicas of data are being stored at different locations, that's why the server cannot completely remove the data on its own. Therefore, it becomes highly risky for the user to put its data on the servers [29].

#### V. Security of Browser

Security of the web browsers has become a serious threat. As a user accesses the data from servers through browsers, so, if the web browser is not secured, all the information can be leaked to a third party [30].

#### W. Data integrity

Since, the data of a user is stored with replicas at different locations, it becomes a serious challenge to provide integrity of data to the user. Data can be modified and corrupted in many ways, thereby, causing the user to lose its valuable and sensitive information

## V. RECOMMENDATIONS

Cloud computing suffers from serious concerns and here some recommendations are provided to address these:

- i) In cloud computing model, the server handles

requests and providing the data to its users all the time. There comes the problem, if due to some reason, the server does not respond, so it cannot provide services in time. There should be an alternative, so that the consumers will not be affected by the server breakdown, and can get timely response.

- ii) Referring to problem 1, there should be a backup plan to recover in case of data loss due to system malfunctioning of one cloud service provider or other reasons.
- iii) There should be some criteria set for cloud services in order to maintain a standardized and error free services.
- iv) As cloud computing infrastructure contains huge data at its servers; therefore, installation, maintenance and up gradation of hardware crucial and extremely necessary for continual
- v) With reference to the problems discussed above, data encryption is the proposed solution. The security loop holes can be covered by proper cryptographic techniques.

#### VI. CONCLUSION

In this paper, architecture of cloud computing, previous research work on it and proposed solutions regarding issues being faced by it have been discussed. Cloud is the future of next generation computing because of the virtualization concept. It is assumed from the success of cloud computing that it will bring numerous developments in IT field hence providing room and scope for research and development in the near future.

#### VII. ACKNOWLEDGMENT

Firstly, I am thankful to Allah for giving us so much courage to study this field of networking efficiently and complete this research paper. Without His help, I would never end up on designing such a protocol. I would like to thank Dr. Muddassar Farooq for providing us with an opportunity to work on this project.

#### VIII. REFERENCES

[1] Shuai Zhang, Shufen Zhang, Xuebin Chen and XiuzhenHuo, "The Comparison Between Cloud Computing and Grid Computing", International Conference on Computer Application and System Modeling, 2010.

[2] Qi Zhang, Lu Cheng and RaoufBoutaba, "Cloud Computing: state-of-the-art and research challenges", The Brazilian Computer Society, 2010.

[3] Muhammad BaqerMollah, KaziReazul Islam and Sikder Sunbeam Islam, "Next Generation of Computing through Cloud Computing Technology", 25<sup>th</sup> IEEE Canadian Conference on Electrical and Computer Engineering, 2012.

[4] Rajesh Piplode and Umesh Kumar Singh, "An Overview and Study of Security Issues & Challenges in Cloud Computing", International Journal of Advanced Research in Computer

Science and Software Engineering, Vol. 2, pp. 115-120, September 2012.

[5] MutumZicoMeetei, "Cloud Computing and Security Measure", 6<sup>th</sup> International Congress on Image and Signal Processing, 2013.

[6] Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", Proceedings of the 44th Hawaii International Conference on System Sciences, 2011.

[7] Flavio Lombardi& Roberto Di Pietro, "Transparent Security for Cloud", SAC'10 March 22-26, 2010, Sierre, Switzerland.

[8] KashifMunir and Sellapan Palaniappan, "Security Threats/Attacks Present in Cloud Environment", International Journal of Computer Science and Network Security, Vol.12, pp. 107-114, December 2012.

[9] Farhan Bashir Shaikh and SajjadHaider, "Security Threats in Cloud Computing", 6<sup>th</sup> International Conference on Internet Technology and Secured Transactions, 2011.

[10] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong, "The Characteristics of Cloud Computing", 39th International Conference on Parallel Processing Workshops, 2010.

[11] Shufen Zhang, Shuai Zhang, Xuebin Chen and Shangzhuo Wu, "Analysis and Research of Cloud Computing System Instance", 2<sup>nd</sup> International Conference on Future Networks, 2010.

[12] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues", In Proceedings of '09 IEEE International Conference on Services Computing, pp. 517-520, 2009.

[13] P. Kresimir and H. Zeljko, "Cloud computing security issues and challenges", In Proceedings of Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, pp. 344-349, 2010.

[14] Jianfeng Yang and Zhibin Chen, "Cloud computing research and security issues", Institute of Electrical and Electronics, 2010.

[15] Yashpalsinh Jadeja and Kirit Modi, "Cloud Computing- Concepts, Architecture and Challenges", International Conference on Computing, Electronics and Electrical Technologies [ICCEET], pp.877-879, 2012.

[16] Akhil Behl and Kanika Behl, "An Analysis of Cloud Computing Security Issues", In Proceedings of World Congress on Information and Computing Technologies, pp. 109-114, 2012.

[17] M. A. Morsy, J. Grundy and Müller I. "An Analysis of the Cloud Computing Security Problem" In Proceedings of APSEC 2010 Cloud Workshop, 2010.

[18] Hanim Eken, "Security Threats and Solutions in Cloud Computing", In Proceedings of World Congress on Internet Security, pp.139-143, 2013.

[19] Maneesha Sharma, Himani Bhansal and Amit Kumar Sharma, "Cloud Computing: Different Approach & Security Challenge", In International Journal of Soft Computing and Engineering (IJSCE), Vol. 2, pp. 421-424, 2012.

[20] Yanpei Chen, Vern Paxson and Randy H. Katz, "What's New About Cloud Computing Security?", Technical Report No. UCB/ECS-2010-5.

[21] Shuai Zhang, Shufen Zhang, Xuebin Chen and XiuzhenHuo, "The comparison between Cloud Computing and Grid Computing", International Conference on computer application and system Modelling, 2010.

[22] <http://securesoftwaredev.com/cloud-computing/resource-pooling/> (Last accessed: 12<sup>th</sup> June, 2014)

[23] <http://www.verio.com/resource-center/articles/cloud-computing-benefits/> (Last accessed: 12<sup>th</sup> June, 2014).

- [24] <http://www.business.qld.gov.au/business/running/technology-for-business/cloud-computing-business/cloud-computing-benefits>  
(Last accessed: 12<sup>th</sup> June, 2014).
- [25] <http://www.rickscloud.com/why-is-cloud-computing-green/>  
(Last accessed: 12<sup>th</sup> June, 2014).
- [26] <http://www.javacodegeeks.com/2013/04/advantages-and-disadvantages-of-cloud-computing-cloud-computing-pros-and-cons.html>.  
(Last accessed: 12<sup>th</sup> June, 2014).
- [27] AfnanUllah Khan, Manuel Oriol, Mariam Kiran, Ming Jiang and Karim Djemame, "Security Risks and their Management in Cloud Computing", 4th IEEE International Conference on Cloud Computing Technology and Science, pp. 121-128, 2012.
- [28] <http://www.javacodegeeks.com/2013/04/advantages-and-disadvantages-of-cloud-computing-cloud-computing-pros-and-cons.html>.
- [29] Sara Qaiser and KausarFiaz Khawaja, "Cloud Computing: Network/Security Threats AndCounterMeasures", Interdisciplinary Journal of Contemporary Research in Business, Vol. 3, pp. 1323-1329, January 2012.
- [30] <https://www.computenext.com/blog/when-to-use-saas-paas-and-iaas/>.  
(Last accessed: 12<sup>th</sup> June, 2014)