International Journal of Recent Research and Review, Vol. X, Issue 2, June 2017

ISSN 2277 – 8322

Security Issues in SPI Models and the Role of Virtualization Technology in Cloud Computing

Salim Ahmad[1], Suleiman Ibrahim[2], Sanjeev Kumar[3]

[1 & 2] Department of Computer Science, Federal University Dutse-Nigeria.

[3]Department of Information Technology, NIMS University, Jaipur, Rajasthan, India.

Email: salim_mgr@yahoo.com

***Abstract* - A cloud computing is a type of computing in which different business processes , data application and information can be stored in the servers owned by third party (cloud Providers) and accessing them through internet services to users, rather than saving and installing them in offices or personal computers. Users can also share the software and other resources on demand. It allows the users to do computing services without the need for them to buy and set up IT infrastructure. The services that are delivered by cloud computing may be accessible worldwide, at low or no cost and based on-demand by users. Cloud computing also delivers different services and deployment models; it also offers some security measures for various services and deployment models. Cloud computing and technology provide individual client/users and organizations with different functionalities to store and process their data in third-party (cloud providers) data centers. The cloud can be used in a variety of different service models comprising of SaaS, PaaS and IaaS which are abbreviated as (SPI) and a known technology which helps is separating the data stored known as Virtualization. The Virtualization technology plays a vital role in cloud computing processes as a technology that supports the entire process of cloud computing and data storage. Therefore, this paper discusses the security issues related to SPI Models and the role of Virtualization Technology in Cloud Computing.**

***Keywords* - Cloud Computing, Security issues, SaaS, Paas, IaaS, Virtualization**

I. INTRODUCTION

The Cloud Computing concept is based on some of the present technologies such as virtualization [1]. Virtualization is the first step towards setting up a cloud. Cloud Computing is having secure access to all your applications and data from any network devices. As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through the adoption of this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered, as the characteristics of this innovative deployment model, differ widely from them of traditional architectures. Cloud computing (virtualization) is a virtual machine that helps to develop the efficiency of cloud computing [1]. With the help of virtualization, it is possible to work on multiple operating systems and applications concurrently over a single server; therefore, virtualization increases the utility and flexibility of hardware.

Cloud computing can be considered as a new computing model that can provide services on demand at a minimal cost. The three well-known and commonly used service models in the cloud paradigm are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In SaaS, a cloud service provider deploys software with the related data, and users can use it through the web browsers. In PaaS, a service provider facilitates services to the users with a set of software programs that can solve specific tasks. In IaaS, the cloud service provider facilitates services to the users with virtual machines and storage to improve their business capabilities [2]. The recent emergence of cloud computing has drastically transformed everyone's view of infrastructure architectures, software delivery and development models. Projecting as an evolutionary step, following the move from mainframe computers to client/server deployment models, cloud computing comprises elements from grid computing, utility computing and autonomic computing, into an advanced deployment architecture. This rapid transition towards the clouds, has driven anxieties on a critical issue for the success of information systems, communication and information security. From a security point of view, a number of unchartered risks and challenges have been introduced from this relocation to the clouds [3].

II. CLOUD COMPUTING SERVICE MODELS

In [4], it is emphasized that there are mainly three service models in Cloud Computing, which includes the following:

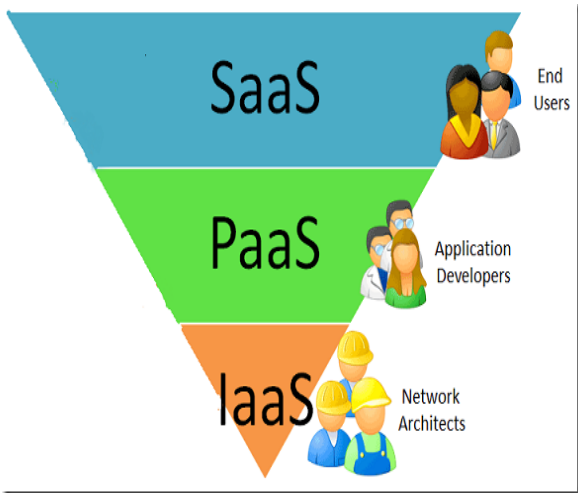

Fig. 1. SPI Service Models (google.com)

A) Software as a Service (SaaS)

Users access the cloud application over internet by making use of interface like web Brower as per requirement and pay for use. It is the duty of cloud provider to sustain the hardware, operating system and application maintenance. Cloud provider offers the security to user as per service level agreement. Many Users can access the application at the same time with their respective subscription. Examples of SaaS are Sales Force, Customer Relationship Services, Google Apps, Gmail, and Google Docs.

B) Platform as a Service (PaaS)

In this type of service model offer operating system and other tools for software development and let user to use its application on the cloud. User does not need to sustain the cloud infrastructure like storage, servers, operating system, programming tool kit, network and software license. User only sustains its software or application and its environment configuration deployed on cloud. Examples of PaaS are Microsoft Windows Azure, Google App Engine, Amazon Web Services, and Elastic Beanstalk.

C) Infrastructure as a Service (IaaS)

In this type of service model, user has direct contact to Central Processing Unit processing, servers, network, and storage devices. User can install and use operating system, software's of their choice on their virtual machines that are accessed through Internet Protocol (IP) address. Cloud provider sustains the basic infrastructure and offers virtualized IP address to the users for direct contact to hardware resources. Examples of IaaS are Amazon EC2, IBM Computing on Demand, Go Grid and Rackspace Cloud.

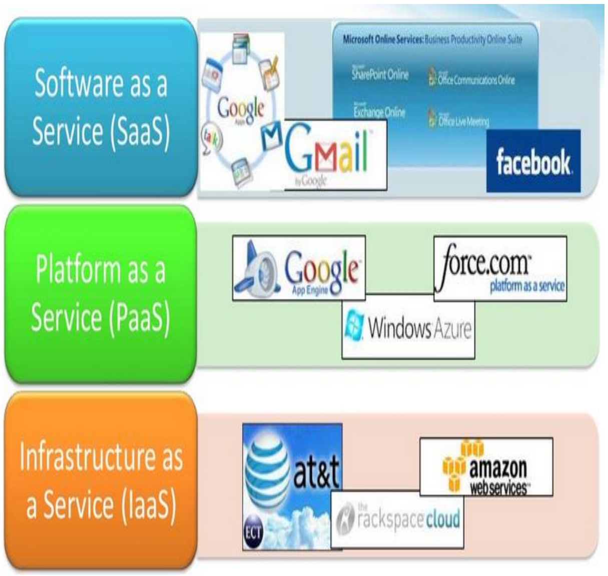
Software as a Service (SaaS)
Google Apps
Gmail by Google
Microsoft Online Services: Business Productivity Online Suite
SharePoint Online
Office Communications Online
Exchange Online
Office Live Meeting
facebook
Platform as a Service (PaaS)
Google App Engine
force.com platform as a service
Windows Azure
Infrastructure as a Service (IaaS)
at&t
ECT
amazon webservices
the rackspace cloud

Fig. 2. SPI Service Model Examples (google.com)

III. CLOUD COMPUTING TECHNOLOGIES

In [5] various technologies of cloud computing as web/server application, database clusters, terminal servers, and virtualization are discussed. The basic concept of Cloud Computing is separating the application from the operating system as well as the hardware its self. This processes of separation brought about the underlying technology of cloud computing called Virtualization. However, [6] identifies many technologies of cloud computing some of which are programming model, data management, data storage, virtualization but in this paper we are focusing on the Virtualization technology with regard to SPI service Models.

Virtualization plays a vital role in cloud computing processes. It is a method of installing and organizing computing resources. It separates the different levels of the application system comprising the hardware, software, data, networking, storage etc. It also breakdowns the division between the data center, servers, storage, networking, data and the physical devices, by recognizing dynamic architecture, then attains the goals of organizing centralized and making use of dynamically the physical resources and virtual resources, improving the flexibility of the system, reducing the cost, improving the service and decreasing the risk of management [7].

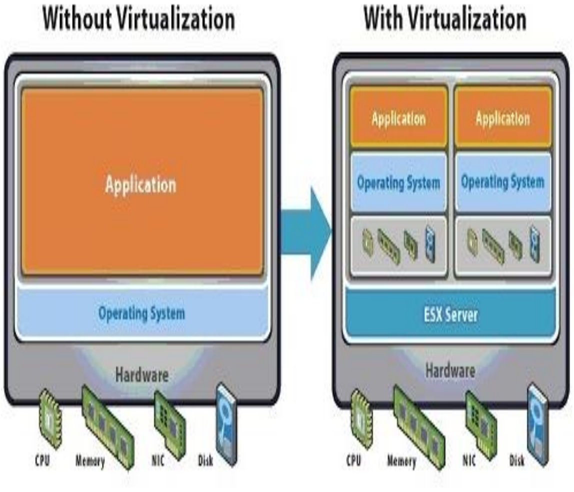

Fig. 3. Virtualization Technology (google.com)

IV. SECURITY ISSUES IN SPI MODEL AND VIRTUALIZATION

According to [8] security issues in SPI models are classified into two different categories: (a) Security issues related to Cloud Service provider and (b) security issues related to customers where the companies stores the data on the cloud and that information can be shared. Therefore, the responsibility of the provider is to make sure that their infrastructure is well secured and the client's data is protected as well with different authentication techniques. When the organization chose to host their applications on the public cloud, the sensitive data is at risk. In order to save resources and for the reduction of cost clouds, service providers often store many clients' data on a particular server. As a result, there is every tendency that one of the user's important data can be viewed by others. To handle such sensitive circumstances, cloud service providers should ensure proper data protection and logical storage [9].

Privacy: Providers must ensure that all private information is encrypted and that only authorized users have access to data. The digital identities and credentials of customers must be protected by the service provider.

Data Integrity: The users always anticipates that the data to be secured and stored in a systematic manner, in the sense that the original data should not be tampered. If the data is corrupted, the user must be able to detect the loss of data and must be able to retrieve the lost data.

Data Accessibility: the cloud service provider must provide the authorization to only users for giving the accessibility to different users in the cloud. All the privileges related to data must be given to only data owner.

In [10-11], it is mentioned that security and privacy is the major issue in both cloud computing models and virtualization, this is because data security has constantly been a major issue in information technology. Data security becomes mainly thoughtful in the virtualization technology in cloud, because data are dispersed in diverse machines and storage devices including servers, PCs, and several mobile devices such as wireless sensor networks and smart phones. Data security in the cloud computing is more complex than data security in the traditional information systems.

V. RESEARCH METHODOLOGY

The techniques used in the research methods are simple questionnaire survey and interviews, the techniques help us in both stages of the research study. The questionnaires were distributed to various respondents with knowledge of how cloud computing works as target audience and the interviews in order to ascertain the level of security issues in SPI models as well as the roles played by Virtualization technology in cloud computing. The empirical part of this paper is based on qualitative and quantitative data collected primarily and secondary. The findings of the results are systematically linked to the theories discussed in the previous section of related literature.

VI. RESULT ANALYSIS

Based on the findings it shows that Virtualization plays a vital role in cloud computing processes, because is a method that enables installations and organizes computing resources. It separates the different levels of the application system comprising the hardware, software, data, networking, storage etc, and also breakdowns the division between the data center, servers, storage, networking, data and the physical devices so as to ensure a hitch free operations in case of server failure or any challenges that may occur in the storage process. On the other hand, security issues in SPI models based on the classifications in relation to Cloud Service Providers and Client's or customer's perspective and agreement have to reach from both parties to ensure the stored data and information can be shared and protected.

VII. CONCLUSION

The security of data is the main issue for any cloud services model. The SPI service providers need to guarantee that the data is effectively protected by making use of different real encryption techniques so that the data can be saved confidentially. Virtualization also helps in separating the data by storing it in different virtual machines so as to retrieve data in case of system failures, also implementing operational data control mechanism supports to keep data safe and secure from unknowns users.

VIII. REFERENCES

[1] Nancy Jain and Sakshi Choudhary (2016) Overview of virtualization in cloud computing. Published by IEEE, in Colossal Data Analysis and Networking (CDAN), Symposium on 18-19 March 2016. Accessed online from: http://www.businessnewsdaily.com/5791-virtualization-vs-cloud-computing.html

[2] Rabi Prasad Padhl, Manas Ranjan Patra, Suresh Chandra Satapathy (2011). Cloud Computing: Security Issues and Resaerch Challenges. Published in IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol.1, No.2, December 2011.

[3] Dimitrios Zissiz, Dimitrios Lekkas (2010) Addressing Cloud Computing Security Issues. Published by ELSEVIER. Future Generation Computer Systems 28 (2012) 583-592. Accessed online from www.elsevier.com

[4] Sapna Malik, MM Chaturvedi (2013) Privacy and Security in Mobile Cloud Computing: Review. published by International Journal of Computer Applications (0975-8887) Volume 80-No11, October 2013.

[5] Rupali R. Kanthe, Ms Rinkle C. Patel (2015) Data Security and Privacy Protection Issues in Cloud Computing. Published in Internatertional Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 3, Issue 2, pp:(1130-1134), Month: April-June 2015, Accessed online on 23rd January 2016, from www.researchpublish.com

[6] Shufen Zhang, Hongcan Yan, Xuebin Chen (2012) Research on Key Technologies of Cloud Computing. 2012 International Conference on Medical Physics and Biomedical Engineering. Physics Procedia 33 (2012) pp:1791 - 1797. Accessed online from www.sciencedirect.com

[7] SeanCarlin, Kevin Curran (2012)Cloud Computing Technologies. Published in International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, No2, June 2012, pp. 59-65 ISSN: 2089-3337. Accessed from

http://iaesjournal.com/online/index.php/IJ-CLOSER/article/view/Northern%20Ireland,%20UK

[8] Shrinivas Adhyapak (2016) An Overview on Cloud Deployment Models and Security issues in Cloud. Published by International Journal of Computer Application (2250-1797) Volume 6 – No. 4 July – August 2016.

[9] Nikita Goel and Toshi Sharma (2014) Cloud Computing – SPI Framework, Deployment Models and Challenges. Published by International Journal of Emerging Technology and Advanced Engineering, Volume 4, Special Issue 1, February 2014, International Conference on Advanced Development in Engineering and Technology (ICADET-14), India. Accessed from www.ijetae.com

[10] Shilpashree Srinivasamurthy, David Q. Liu, Athanasios V. Vasilakos, and Naixue Xiong (2013). Security and Privacy in Cloud Computing: A Survey. Parallel & Cloud Computing.2 (4), 126-149. New York, NY: American V-King Scientific Publishing, LTD. http://opus.ipfw.edu/compsci_facpubs/44

[11] Sean Carlin, Kevin Curran (2012)Cloud Computing Technologies. Published in International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, No2, June 2012, pp. 59-65 ISSN: 2089-3337. Accessed from http://iaesjournal.com/online/index.php/IJ-CLOSER/article/view/Northern%20Ireland,%20UK