VOL 2 (2018) NO 4 - 2

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

A Review on Cloud Computing Security

Marry Teo[#], Hairulnizam Mahdin[#] , Lee Jia Hwee[#], Haezel Ann Dicken[#], Tay Xin Hui[#], Teng Mee Ling[#], Mohd Sanusi Azmi[*]

[#]*Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Malaysia*

[*]*Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Melaka, Malaysia*

Email : ai150172@siswa.uthm.edu.my, hairuln@uthm.edu.my, ai150177@siswa.uthm.edu.my, ai150007@siswa.uthm.edu.my, ai150165@siswa.uthm.edu.my, ai150174@siswa.uthm.edu.my, sanusi@utem.edu.my

***Abstract*— Cloud computing is a technology that maintain the data and application by using the central remote server with the internet connection. By utilizing cloud computing, user can reduce their costs as they no need to purchase their own hardware and software. However cloud computing still has many issues concerning securities, such as privacy issues, loss of data and stolen of data. Some security issues over cloud services including confidentiality, integrity, availability, privacy and attacks are concerned by the users. This paper reviews some of the issues and its current solutions.**

***Keywords*— Cloud computing, security**

I. INTRODUCTION

Cloud computing drives the current computing tendency by providing a flexible facility or services over the cloud. Cloud computing is an on-demand computing service which enables the user to store and get right of entry to their data over the Internet [1]. In brief words, cloud computing is technology, storage provision, and hosting platform combined that can be found on the Internet [2-4]. In terms of marketing, it provides services without end user knowledge about where is the physical location at and configuration of the services provided. It provides a cloud platform to add capacity and capabilities without concern on the infrastructure investment, training IT personnel or licensing new software. It allows consumers and businesses to access their files anytime at anywhere without any installation software but it requires internet connection to access. Scalability, affordable on-demand infrastructures of computing, and good service quality levels are the main goals of cloud computing [3]. Nonetheless cloud computing has many circulations concerning securities, such as privacy issues, loss of data and stolen of data. Although there are voluminous of companies in the current market that develop and offer cloud computing services and commodities, most of them are still unaware of the repercussions of storing, processing and accessing data in an enormously-shared and virtualized location [4]. This lead to user cannot realize how the service provider oversees their information or indeed where their information is put away. Therefore, there are a lot of question will be come out like "Why I want to believe the third party?" and "Is it secure for the location to keep the data information?" As a result, there are some consumers are not willing to adopt the cloud services although it brings a lot of advantages to them. When in reality, security is the biggest complication that cloud-based developers failed to include in their services. As cloud computing explodes in the Information Technology (IT) market, security issues faced by cloud providers and customers became important. Additionally, regardless of the current affordable technologies that are capable of handling securities, some developers still could not deliver the best of security in their services. This make the cloud services provided suffers from a few of vulnerabilities such as it is easily to be attack from attackers who would like to obtain a free computing service, information theft from cloud users and penetration of the infrastructure through cloud connection. There are some considered reasons such as the company will be lost the control on the data since they host their assets by using outsourcing security management in a third party [5]. Another reason is lacking security guarantees in the Service Level Agreements (SLAs) between the consumers and the providers [6]. Thus, cloud providers must ensure a secure infrastructure and protect client's data and applications. Customers must confirm providers on the security steps taken to protect their data.

The rest of the paper is organized as follows: in Section II, the theory of the cloud computing will be discussed in detailed. Literature review will be explained in Section III.

In Section IV, the result of the analysis of security problem will be discussed. Finally, Section V is the conclusion.

II. LITERATURE REVIEWS

A. *Type of services*

All of the cloud services have their own service providers, service providers are companies that offer a few components of cloud computing to the business or individual [7]. Cloud computing is build up by three different layered. Infrastructure of a Service (IaaS) is the first layer that permit user to borrow the process, capacity and diverse essential computing assets to set up and run the arbitrary software program which consisting of operating system and applications. The second layer is Platform as a Service (PaaS) which gives a platform for user to implement and run their applications. Software as a Service (SaaS) is the third layer of cloud service model. It is a complete software application which can be specifically utilized by end user through different devices such as web browser. It is easier to be used when compared to the traditional service as user no need to download and install on their laptop. Cloud deployment models have differentiated into various types which are public, private, hybrid and community cloud. Public cloud is a cloud that made accessible to the general public and is owns by an organization who offering the cloud services. Public cloud can be accessed by any subscriber. It is based on pay-per-use model and less secure compared to other cloud. Private cloud is utilized for a single organization either by inside or remotely hosted. Users can share and use the provided resources and virtual application. It is based on the concept of intranet functionality and thus more secure. Hybrid cloud is the cloud that combines two or more clouds such as public cloud or private cloud which are bound together advertising the benefits of numerous deployment models. Hybrid cloud can be accessed by various parties and has a more secure control of the data and applications. The open architecture features allow interfaces with other management systems. Community cloud is shared by a few organizations and usually used remotely hosted.

B. Technologies

Since cloud computing comprises of various technologies such as virtualizations, databases, transactions, networks, load balancing, operating systems, resource scheduling, memory management and concurrency control, there are abundant of security concerns in cloud computing [8]. These technologies and systems have many security issues that are related to cloud computing. For instance, quite a few numbers of security concerns were resulted in cloud computing concerning virtualization, and networks must be kept secured in order to interconnect the systems in the cloud. Additionally, mapping of the corporeal machines and the virtual machines must be carried out in a secure matter. Besides, data security emphases on data encryption and also the suitable policies are ensured to be enforced for data sharing. Additionally, memory management and allocation of resources algorithms must be in a secured condition, and the detections of malware in clouds must be applicable in techniques of data mining.

Cloud computing components consist of client, data center and distributed server. Client is divided into three types which are mobile device, thin client and thick client. Thin client is the most popular as it is cheaper, less security issues and low failure and data lost possibility. Data center consists of a collection of server that stores data and software. Distributed server gives options and security flexibility to cloud providers. There are two types of categories in security threats model which external and internal threats. External threats include Dos, DDoS, port scanning, IP spoofing, DNS poisoning, phishing and packet sniffing. Internal attacks involve an attacker as an insider to access user's resources. Besides, there are nine types of threats in cloud computing which are changes to business model, misuse of cloud computing, insecure API interfaces, malicious insider, multi-tenancy nature, data theft, service hijacking, risk profiling and identity theft. Changes to delivery of IT services can be solved by end-to-end encryption and trust management scheme. Proper validation/verification and stronger authentication can be used to handle misuse of cloud computing. Proper security model and access control mechanism can be implemented to settle insecure API interfaces. For malicious insider, transparency and management are required to avoid the risk. SLA patching is vital to help in shared technology issues in IaaS. Loss of control to data should be mitigated by security of API, data integrity, data backup and so on. Service hijacking, risk profiling and identity theft can be solved by using security policies, monitoring and alerting system and strong authentication respectively.

C. Cloud security architecture

Cloud security architecture only can effectively secure the cloud services from threat if and only if the correct defensive steps are carry out at the correct place. Cloud security control act as a safety guard on the weakness of cloud and reduce the loss of the attack faced. Indirectly, this control help to reduce the attacks on the cloud computing. These controls include deterrent controls, preventive controls, detective controls and corrective controls. Security control increases the safety level of data in cloud services. Besides, when discuss about the data security, few security requirements need to consider preventing any attack on cloud computing service. Security requirement such as data availability, data confidentiality, data privacy and data integrity control over data accessing by different parties to reduce the risk of any abuse of the data in cloud computing. Availability is defined to ensure that users can use the infrastructure, software and data anytime at anywhere [9]. With the internet connection, it allows the users to access to cloud to retrieve data, service or infrastructure. Redundancy is a technique to provide the availability in cloud since it stores multiple copies of similar data [10]. It increases the searching speed and reaches availability of the system. Next, confidentiality and privacy is important [11]. The data of user should not be disclosure to any unauthorized third party. Only the authorized user can access to the system for retrieving data. In order to enhance the confidentiality, encryption of the data should be implemented. Homomorphic Cryptography performed on an encrypted text [12]. When storing the cloud data, the data can be stored at any location in the world and it has to follow the privacy and confidentiality laws of the country that the server is located.

In order to improve the security, Two-Factor authentication solution should be implemented in order to avoid the breach in privacy. Integrity is not only related to edit or modification of the stored data but also the data lost and stolen. It is a key aspect of security in cloud computing system.

III. Security Concerns

According to [13], security issues always become the concerned in cloud computing as nowadays people always storing their important data inside the cloud because of easy to access at anywhere and anytime. Hence, cloud service provider must make sure that user's information is secure and without confronting any issues such as information loss or information burglary which may cause an incredible loss. Security issues and challenges upraised in cloud computing included data issues, security issues, privacy issues, application issues, threat issues. The most common security issues in cloud computing is data theft. Data issue has emerged majorly with regards to security in cloud computing with reference to sensitive data. At any time that a data is available in a cloud, anyone with access to the Internet can retrieve the data from anywhere given that data could be shared, private and sensitive in a cloud. Consequently, many users and provider of cloud services have access to these data and can manipulate them as well. Thus, data integrity steps need to be taken in cloud computing. Not only the reason of data theft, some of the cloud service providers don't have their possess server also cause the security issues in cloud computing where it must two user levels namely cloud service provider level and customer level. All servers should be kept safe from any external risks should be made assured by service providers, while the customer should be aware of any data loss or interference of data. For privacy issues, customer's personal information and data must be made well secured by cloud service providers from the reach of other users, customers and providers. Cloud service provider must be authenticated the user who access to the data stored in the cloud is the right people and only the authorized user can get the right entry to the data [14]. For application, issues, cloud service provider is responsible to monitoring and maintenance the application in order to make sure that it is secure and not tainted by any pernicious code which can harm, modified and stolen your information inside the cloud. Means, service providers should have full access to their servers, which can help prevent any unauthorized users to upload infected application into the cloud, resulting in affecting the cloud service and customers' data. There are nine threats should be concerned in order to prevent the threat issues happened which including information breaches, information loss, account capturing, uncertain APIs, Denial of Service, malicious insiders, mishandle of cloud service, inadequately due diligence and shared technologies issue [15]. The top reason that caused the information loss is hardware malfunction and second is human blunder.

Based on 16], some security issues include confidentiality, integrity, availability, privacy and attacks. Data security remains an ambiguous issue as sensitive data may become untrusted after transferring to cloud. Unexpected incident like loss of control over IT services and insider threats or attacks may occur. A few key elements of security issues in SaaS, PaaS and IaaS considered which are data security, data confidentiality, authentication and authorization and so on. Cloud providers cover the scope of security below the application level in PaaS. Hackers may attack the infrastructure and perform extensive black box testing. IaaS store applications and sensitive data in cloud environment by using virtual machines. There are many possible security attacks include Denial of Service (DoS) attacks, side channel attacks, authentication attacks, man-in-the-middle cryptographic attacks and network security.

Based on [17], there are seven types of attack which include zombie attack, service injection attack, virtualization attacks, man-in-the-middle attack, metadata spoofing attack, phishing attack and backdoor channel attack. Zombie attack interrupts availability and cloud behaviour. Better authentication, authorization and IDS/IPS can be used to solve it. Service injection attack can be defended by using service integrity checking and strong isolation between VMs. Virtualization attacks perform by VM Escape and rootkit in hypervisor. IDS, IPS and firewall can be used to handle virtualization. Man-in-the-middle attack access the data exchange between two parties. SSL configuration and data communication tests are recommended to defend the attack. Spoofing attack usually modifies or changes the service's Web Services Description Language (WSDL) file. Customers should keep an encrypted form of information to overcome it. Phishing and backdoor attack can be mitigated by strong authentication.

As stated in [18], Deterrent controls are the controls help in reducing the attacks on cloud computing. Deterrent controls will be warning the attacker as they will take the consequences if they continue to proceed with their attack. This control will reduce the threat level and give warning sign on the fence to the attacker. Preventive controls are the controls that reduce the vulnerability through strengthen the system against the incident that might happen if the control cannot completely eliminate the vulnerability. One of the methods is having strong authentication to reduce the probability of attacker to have unauthorized access to sensitive data while the users are positively identified at the same time. Third control, detective controls aimed to take action on incident occurs. Detective controls will detect and react to the attacks and signal the preventative controls or corrective controls to take appropriate steps to work out on it. For the instant, intrusion detection and prevention arrangements are used to detect attacks on the cloud system. Lastly, corrective controls are controls that take over steps to reduce the damage and effect of an incident on the system. Restoring system backup is carried out as a step to have corrective controls on the incident happen. These controls will affect the effectiveness of the security and architecture of the cloud system.

The aim of data confidentiality is to make sure the data is only available to the authorized user especially the sensitive data and disclosed to illegal users. The only owner of the data can fully access the data in cloud computing without the leakage of the data content to other parties. Property of data access controllability allows data owner to make use of the selective restriction of access to his data outsourced to cloud [18]. Only the parties allowed by data owner can access the

data through fine-grained access control over outsourced data. This control ensures each party who allowed to access to the outsourced data using different access privileges with regard to different data pieces [18]. The owner must take over the control of the data especially in untrusted cloud computing environment to prevent any possible loss. While data integrity protects the data from any modifying, deleting, fabricated or illegally tampered by other parties. This requirement allows the accuracy and completeness of the data and having correct and trustworthy of the data stored in the cloud system. If there have any incident happen to data either deleted or corrupt, data owner able to detect it and get back the lost data. Various security threat such as virtualization vulnerability, side channel attack, abuse of cloud services and others threat can be prevented under these requirements and limit the lost over the data stored in the cloud system.

Cloud computing in security perspective is a concerned issue and has been discussed from various researchers. The use case scenarios and related requirements that possible happens in the cloud computing model are discussed. The consideration of use case includes the consumers, developers as well as security engineers [19]. In another research, ENISA the vulnerabilities and impacts are the risks that related to the adoption in cloud computing and is very concerned by the consumers [20]. Different security risks are investigated in the research paper. Similar efforts to CSA, "Top Threats to Cloud Computing" is discussed and best practice are delivered from cloud provider, consumers and security vendor [21].

IV. DISCUSSIONS

Cloud computing allows user to choose what information they have access to within the cloud. It provides cloud storage for user to store information and use the computer resources. This in turn helps entrepreneurs and companies to cut cost in purchasing hardware or other devices. Cloud computing provides flexibility on request over the network. It is location and hardware independence and resources are occupied by many users at a time. It further provides reliability, security and maintenance to users. How to choose cloud providers? SaaS provides convenience for users to acquire the same software on all of your devices at once. It has the least control in SaaS agreement. PaaS gives subscribers access to the components and operate applications over the internet. IaaS make users outsources the storage and resources.

There are several solutions and practices have been discussed in order to extend the safety in cloud computing. Firstly, cloud service provider should take a look at the defencelessness of their cloud service regularly and must continuously keep up and update the cloud to limit the attainable get to point and must be diminish the hazard that can give the opportunity for hacker to attack your service. Secondly, trusted cloud service provider should be always chosen by user such as Google, Microsoft and IBM. User should think properly before chosen the cloud as distinctive service provider have diverse approaches on manage the data information in the cloud. Besides that, all of the information store within the cloud should be encrypted well in order to extend the security of the data. No one can get to the information on cloud without permission, service provider must be make sure that user access is the one who storing the data. Other than that, user should understand clearly about the security condition of data on cloud, user is responsible to contact the service provider before using it. Cloud service provider should always backup the user's data in order to make that if data loss accidently occur, they can directly recovery the data of the users. Users access to their data on cloud not only authenticate by username and password but also digital data. Single Sign-on enables user to access multiple applications and services through a single login and enabling strong authentication. Security defence can be installed which include virtual private networks (VPNs), virtual local area network (VLAN) segmentation, authentication, Intrusion Prevention Systems (IPS) and intrusion detection systems (IDS). Cloud availability can be done by active/active clustering, dynamic server load balanced and ISP load balancing within the network infrastructure. Data loss prevention (DLP) tools can be used to increase data privacy and CSP (cloud service provider) can be used for data integrity. Virtual Machine Protection functions by isolating and inspecting other network segments.

Identity and Access Management and Federation is one of the enabler to improve the cloud computing security. The main security aware system is called Identity. It helps to differentiate the users, services, servers, cloud and other entities by system because it consists of a set of specific entity information associated [11]. Cloud platform should not only private all user personal data but also build a boisterous and logical Identity Management System which hides all the context information of cloud objects and cloud users. Secondly, one the key objectives of the cloud computing security (CIA) triad are called confidentiality. By encrypting all the data, it helps to achieve the confidentiality objective. Encryption algorithms are using either symmetric key or asymmetric key. However, there is a main problem on generating, storing, accessing and exchanging the secret keys. The key must be maintained securely along in order to access the APIs. Next, security management plays an important role in cloud computing security. Due to the increment on number of cloud stakeholders, the larger number of security controls and makes the cloud security management to be a more complicated research problem. Security requirements and policies specifications, configuration and feedback are necessary to the security management [20]. Moreover, the cloud-based application uses the secure software development lifecycle to build a secure system. In order to help developing secured cloud-based applications, the PaaS provide security components which are reusable. Service Level Agreements (SLAs) helps in security performance trade-off optimization. Performance, reliability and security are the objectives of implementing the SLAs. Trade-off between security and performance should be considered by cloud management [19].

Another solution for security issues is a layered framework of cloud security is proposed to assure that the security in cloud computing can be made better. The first layer is stacked at the bottom which is the secure of virtual machine layer. The second layer is the cloud storage layer, which in order to construct an immense virtual storage, this

layer provides an infrastructure that can combine resources from multiple of cloud service providers. The fourth layer, cloud data layer, handles the problems for instance key logger XEN [8] to help combine together software and hardware solutions in virtual machines.

The performance of an effective and reliable service to meet the needs mentioned under and within the maximum transaction system boundary conditions [22]. Performance control and analysis techniques are required to process big size data in the cloud computing because the performance of the cloud computing will affect the number of users over cloud services. Several criteria such as SaaS, PaaS and IaaS that can affect the performance of the cloud computing need to be consider when evaluating the performance of cloud services. Performance of the SaaS can directly evaluate through the speed of response, reliability of technical services and availability [22]. PaaS can either evaluate directly or indirectly over response to technically, productivity, reliability, technical service and middleware capability [22]. While IaaS is depending on infrastructure performance, capacity, reliability, availability and scalability [23]. For the service provider, they can measure the performance of the cloud computing through delay in service and accuracy. Level of service or called Quality of Service (QoS) in Service Level Agreement (SLA) will indicate the level of performance and reliability over response time, productivity, availability, and security of the cloud services. Speed is the time interval for a function to operate successfully which show the level of performance at which the security is achieved at the same time. However, the performance will be affected by the resources, disk space, bandwidth, CPU speed, memory and network connections.

The efficiency of cloud computing can be measure through security and performance in a security system. Security is an element to protect the system from threats while performance indicates the speed of processing the data to and fro from different nodes. Security of the cloud computing will affect the level of performance because threats will affect the functionality of certain part of the cloud system and low functionality will have low performance. Security is one of the system efficiency factor and efficiency is the main consideration in performance. Thus, both performance and security depend on each other in the development of the system. In SLA, the service provider should make security available to user but user will be a security breach if he did not follow the security policy. In this case, user leads to low security of the system that will directly affect the performance of the system. In other hands, security affects the performance of the cloud system while performance affect by the user and service provider and the component of the services affect the security.

V. CONCLUSIONS

Cloud computing is becoming popular in this technology world. People are likely to store their data on the cloud because it is convenient for them to access their data anywhere and anytime over the internet. However, security issues are becoming the challenges for service provider. In order to have a resilient and joint understanding between the cloud service provider and the customer, both of these users should make sure that the cloud they use is secure enough from any outside threats and no other parties can be access without permission. It is important for service provider to find out more defense approach to reduce the security issues arise. Cloud security has a large gap between its practice and research which is the assumptions in the research that overlook some very crucial differences between virtual machine security and the actual cloud security. Research should be the bridge of these gaps. One layer of the framework might help in coming out with a solution to monitor the management of the cloud software and another layer might help in solving the secluded processing for a particular client's application. In order to deliver the integrated security, the integration and combination with other security controls at different layers should be supported. Cloud computing security should be able to change the environment by following the demands of stakeholders. Multi tenancy protection should be implemented which only allow the user to view his own security configurations.

REFERENCES

[1] Griffith E. (2015). What is cloud computing? [Online]. Available: http://sea.pcmag.com/networking-communications-software/2919/feature/what-is-cloud-computing

[2] Lamba, Harjit Singh, and Gurdev Singh. "Cloud Computing Future Framework for e-management of NGO's." *arXiv preprint arXiv:1107.3217* (2011).

[3] Singh, Gurdev, Shanu Sood, and Amit Sharma. "CM-measurement facets for cloud performance." *International Journal of Computer Applications* 23, no. 3 (2011): 37-42.

[4] Schaper, Joachim. "Cloud Services." In *Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on*, pp. 91-91. IEEE, 2010.

[5] Mathkunti, Nivedita M. "Cloud Computing: Security Issues." *International Journal of Computer and Communication Engineering* 3, no. 4 (2014): 259.

[6] Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[7] Ashraf, Imran. "An overview of service models of cloud computing." International Journal of Multidisciplinary and Current Research 2, no. 1 (2014): 779-783.

[8] Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security Issues for Cloud Computing." *International Journal of Information Security and Privacy* 4, no. 2 (2010): 36-48.

[9] Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and Muttukrishnan Rajarajan. "A survey on security issues and solutions at different layers of Cloud computing." *The journal of supercomputing* 63, no. 2 (2013): 561-592.

[10] Singh, Saurabh, Young-Sik Jeong, and Jong Hyuk Park. "A survey on cloud computing security: Issues, threats, and solutions." *Journal of Network and Computer Applications* 75 (2016): 200-222.

[11] Almorsy, Mohamed, John Grundy, and Ingo Müller. "An analysis of the cloud computing security problem." *arXiv preprint arXiv:1609.01107* (2016).

[12] Arora, Rachna, Anshu Parashar, and Cloud Computing Is Transforming. "Secure user data in cloud computing using encryption algorithms." *International journal of engineering research and applications* 3, no. 4 (2013): 1922-1926.

[13] An, Y. Z., Z. F. Zaaba, and N. F. Samsudin. "Reviews on security issues and challenges in cloud computing." In *IOP Conference Series: Materials Science and Engineering*, vol. 160, no. 1, p. 012106. IOP Publishing, 2016.

[14] Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security issues for cloud computing." *Optimizing information security and advancing privacy assurance: new technologies: new technologies* 150 (2012).

[15] Kandias, Miltiadis, Nikos Virvilis, and Dimitris Gritzalis. "The insider threat in cloud computing." In International Workshop on Critical Information Infrastructures Security, pp. 93-103. Springer, Berlin, Heidelberg, 2011.

[16] Basishtha, S., Boruah, S. “Cloud computing and its security aspects.” *International Journal of Research in Engineering and Technology. (2013):* vol 2(2), 62-67.

[17] Kashif Munir and Sellapan Palaniappan. “Security threats/attacks present in cloud environment.” *International Journal of Computer Science and Network Security*, (2012): 12(12), 107.

[18] Mahesh B. “Data Security and Security Controls in Cloud Computing.*”* *International Journal of Advances in Electronics and Computer Science*, (2016): 11-13.

[19] Inukollu, Venkata Narasimha, Sailaja Arsi, and Srinivasa Rao Ravuri. "Security issues associated with big data in cloud computing." *International Journal of Network Security & Its Applications* 6, no. 3 (2014): 45.

[20] Stojmenovic, Ivan, and Sheng Wen. "The fog computing paradigm: Scenarios and security issues." In *Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on*, pp. 1-8. IEEE, 2014.

[21] Ahmed, Monjur, and Mohammad Ashraf Hossain. "Cloud computing and security issues in the cloud." *International Journal of Network Security & Its Applications* 6, no. 1 (2014): 25.

[22] Zanoon, N. “Toward Cloud Computing: Security and Performance*”*. *International Journal on Cloud Computing: Services and Architecture*, (2015): 5(5/6), 17-26.

[23] Shailesh Paliwal. (2014) Performance Challenges in Cloud Computing. [Online]. Available: https://www.cmg.org

[24] Ashraf, Imran. "An overview of service models of cloud computing." *International Journal of Multidisciplinary and Current Research* 2, no. 1 (2014): 779-783.