IJCTA, 9(12), 2016, pp. 5695-5702

Survey on Analysing the Cloud Security Discrepancies with Performance Measures

***R. Balamanigandan **Dr. K. Krishnamoorthy ***M.Uthaya kumar**

Abstract : Security and privacy concernsare shown to be the primary obstacles to a wide adoption of clouds. The new concepts that clouds introduce, such as multi-tenancy, resource sharing and outsourcing, create new challenges to the security community. Security has become the greatest obstacle and booming revolution in Cloud Computing, which occupies the top concern in the minds of the researchers. In this paper provide a comprehensive method of cloud computing security and privacy concerns and identify cloud vulnerabilities, classify known securitythreats and attacks, and present the state-of-the-art practices to control the vulnerabilities, neutralize the threats, and calibrate the attacks.Cloud Computing is the master of IT services, providing platform for delivering the requirements on demand and paid based on the service accessed over the internet.It is the paradigm which cannot be resolved for its unimaginable activities; this allows users to make use of an application at any location or devices. Confidentiality, Integrity, Privacy of the data residing in cloud storage is the concern that is yet to be solved. So, a lot of research activities is been prompted by these issues, aiming to cover the pitfalls of the security leaks.This paper exaggerates the vulnerabilities that occur maintaining in the data integrity and a proposed model to protect the user data in a shared pool of computing resources and also we converse here on spotting the major vulnerabilities in this type of structures and the largest part of essential threats found in the literature related to vulnerabilities and threats with probable elucidation.

Keywords : Cloud Computing, Confidentiality, Data Integrity, Security, Privacy.

1. INTRODUCTION

Cloud Computing is often called as a service deliverer over the internet which is provided on- demand. The cloud computing infrastructure renders a valuable concrete for accessing the applications anywhere and anytime. It clings to service providers to distribute a shared pool of resources, networks, computing capability of processors and storage space. Clouds at its various perspectives are elaborated in the following research. The adorable features of cloud computing includes delivery of on-demand service which can be elaborately explained as availability ofrequested service can be obtained at any instant of time with the maintenance of own computing resources . The services by cloud providers are available through public, private, community, hybrid cloud (Gkatzikis et al 2013). The services provided by public cloud are offered over the internet and managed by the cloud providers. In this type of cloud, it would be maintained by a private organization. The services are organized by a cloud provider among the particular community which consists of culmination of many firms in groups and the services are shared over internet based on the requirements of the groups. It is the combination of different existing cloud models.Cloud Computing is dynamically scalable and has virtualized resources which provide various services that are exhibited as follows: As depicted in Figure 1 the following cloud services are explained, In SaaS, an already made application along with the software and hardware are provided e.g., Microsoft Office365. In PaaS,

* Assistant Professor, CSE, Sri Krishna Engineering College, Research Scholar, Karpagam University, Coimbatore. bala16385@gmail.com,

** Professor & HOD Department of CSE, Sudharsan Engineering College, Pudukottai, Tamilnadu, India. kkr_510@rediffmail.com, Assistant

*** Professor, Department of CSE, Bharath University, Chennai, India. uthay.proff@gmail.com

an environment is provided along with the hardware, software, operating system and networks to deploy own application parameters e.g., Amazon Web Services (Khan et al. 2014). In Fig1 IaaS, hardware and software are provided with which own applications and operating environment can be deployed *e.g.*, Windows Azure.

The basis for the popularity of cloud Computing includes; Low initial capital investments, new services can be started in a short span of time, Less maintenance and operational costs, Virtualization, (Jiadi Yu et al) on-demand delivery of services, Pay-for-use, Scalability, reliability, efficiency. The limitations and challenges are depicted as follows; the privacy and security are the greatest concerns of cloud computing whose performance are still a demanding subject today. The data that is shared over the internet is often tends to be insecure due to the fact that they are stored in a remote location. Because the cloudproviders have multiple clients accessing the services simultaneously and it is very difficult to control. As a result of exposure the data loses its intergrity. Security breach

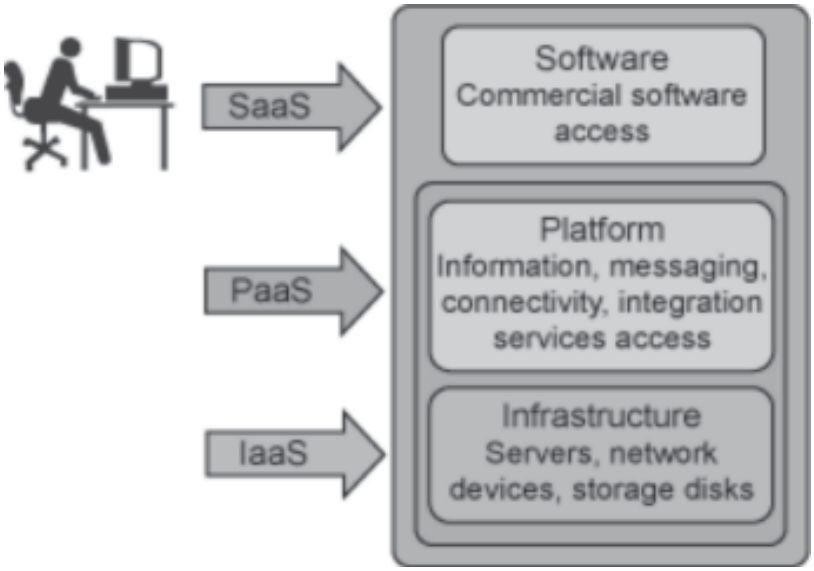

Fig. 1. Cloud Computing Services Models

arises when the data is not protected properly from the third party. To provide a better and protetive services certain contracts and reviews should be tracked properly to avoid hacking (SoaresBoaventura et al).In today's era, two-third of this world tends to adopt this pervasive environment including the business and information based companies. Among those 88% of users say that the acquirement of cloud services would be made evasive if the cloud security also could have been better. Still security remains as the top most concern and barrier for the users. So, this plays a major role in slow adoption of cloud services (QiangDuan et al). Despite the public cloud offers low investment of cost, the people as well as the organizations opt to choose the private cloud environment for the security compliance and reasons. When more and more information or data is kept in cloud by the organizations and people, the question arises on how the security will be provided. It is analyzed that; when an argument arises, where the data will be secured? Most of them raise their support for personal storage (Jens-Matthias Bohli et al). The cloud storage data cannot be secured properly because, they do not employ high levels of security and it is distributed in the open environment regardless of the how important the content is. The Cloud Computing has many attractive features like availability, flexibility, cost effectiveness, etc. But, it has certain challenges which have to be taken in account. In the context of public cloud, all the service structures like IAAS, PAAS, SAAS has the inter-operational characteristics.Cloud computing infrastructure is changing fast requiring security measures and policies to be updated regularly at the same pace to match the changing behavior of the clouds. Furthermore, Figure 2 refers about licensing is crucial to the security of clouds. Standard policies should be strictly implemented in clouds and organizational/governing bodies should visit clouds' staff and infrastructure on regular bases to evaluate the efficiency of the security precautions adopted by the vendors. This is a greatest hindrance for accepting cloud services. A way to reduce the risk factors of data corruption and applications may be avoided by using multiple clouds.

Many methodologies and systematic approaches were introduced and used. The following paper work elaborates on the various security issues and crisis, and a methodology is proposed to safeguard the data in the cloud for valuable consumers.The main objective of this proposal includes a list of vulnerabilities and threats, and we also point out how cloud service models can be affected by them. In addition to that, we portray the affiliation between these vulnerabilities and threats; and in the way in which these vulnerabilities can be subjugated to perform an attack, and also in attendance some counter measures interrelated to these threats which attempt to improvise the recognized problems.

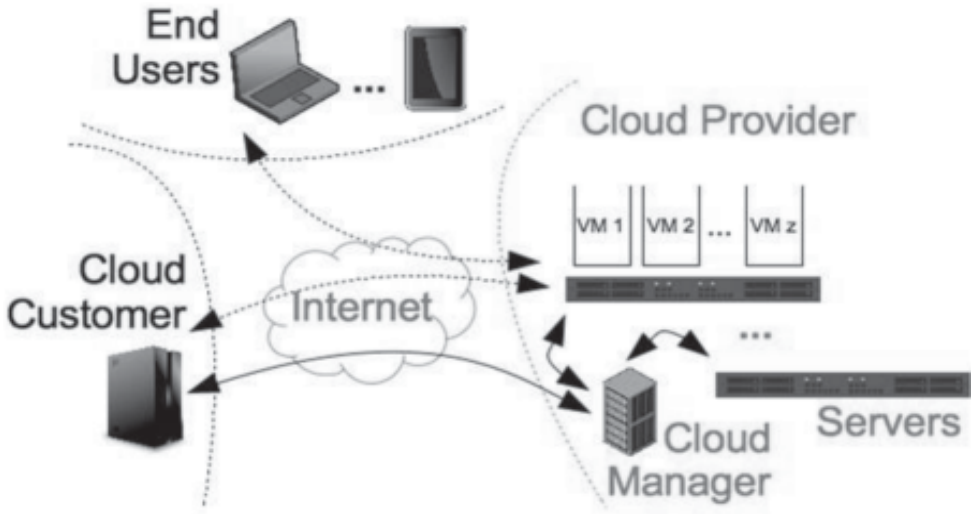

Fig. 2. Cloud Computing Design and Services

Materials and Methods

There are lots and lots of features and brilliant characteristics' that attract the industries, various organizations and individuals towards the revolutionary functionalities of cloud computing. The virtual aspect of cloud migrates and penetrates the work of most concerned organizations. In these days Salesforce, Amazon, Google are providing on-demand delivery of services on pat-by-use basis. There are many vendors collaborating with the service providersand it is totally based on the users' interest to choose the vendors and the application. It is purely based on users' perception and usage (Jens-Matthias Bohli et al). Despite the services offered, there are also security breached involved it in for the user account and data that is stored in cloud. The various security challenges in cloud are depicted in the following scenarios.

The large cloud service providers have their data centers spread worldwide. So, the users have the option of storing the data in public cloud in any region, but integrity cannot be assured many a times. Next issue is the access rights that are shared among the consumers; the potential hackers can intrude the credentials and the stored information. Apart from this Service Level Agreements (SLAs) and Policing between the customers and the service providers snoops the details of the uploaded information. The crucial scenario in cloud computing is that, it implicitly encloses the sensitive personal and business information and processes. So, the consumers must be made aware of the protection and control atmosphere. Hence, a well-built relationship should be made legally between the consumers and the service providers. If the intruder breaches the security aspects of a particular consumer's storage area, then he might be able to make alteration in the original data available. This can probably be done or carried out any number of times by the intruder. He can also acquire the rights to access the logic of the cloud and change the input and output functionalities.

1. Taxonomy of security breaches in cloud computing

Security is considered to be the major factor for the feasible use of cloud computing. Since there are many consumers interested in having business in cloud servers, there is need for explicit technology for the security credentials to be maintained effectively.They are many security problems involved in various layers of the cloud that has to be rectified. Despite, Figure 3 explains the concept of virtualization and service oriented architecture provides a very eminentplatform for cloud applications, but the huge issues stands as a barrier for customers to adapt those fields. The important security issues in cloud computing are discussed below subtopics;

Fig. 3. Unauthorized Accessing of Cloud Data

2. Security violation in cloud computing layers

The cloud computing stack consists of the services layers like IAAS, PAAS, SAAS, which are the most targeted parts of security or hacker attacks (Kevin Hamlen et al);

(*a*) Security Issues in SAAS

The following are the security issues in the layer Software as a Service :

1. Security issues in the data that is uploaded.
2. Security crisis in the network platform.
3. Intrusion of locally residing data.
4. Integrity Prone System.
5. Unauthorized Data Access.
6. Breach in Web Applications Security.
7. Vulnerabilities in Virtualization

(*b*) Security Issues in PAAS

The platform as a service is the layer which offers the environment for the user or customer to develop code based on the application he is developing :

1. Network intrusion is the biggest concern in this layer.
2. Hackers can easily abduct the code from the host layer.
3. Cross VM attacks.
4. Redundancy.

The Fig. 4 explains solutions and approaches for security issues in cloud layers.

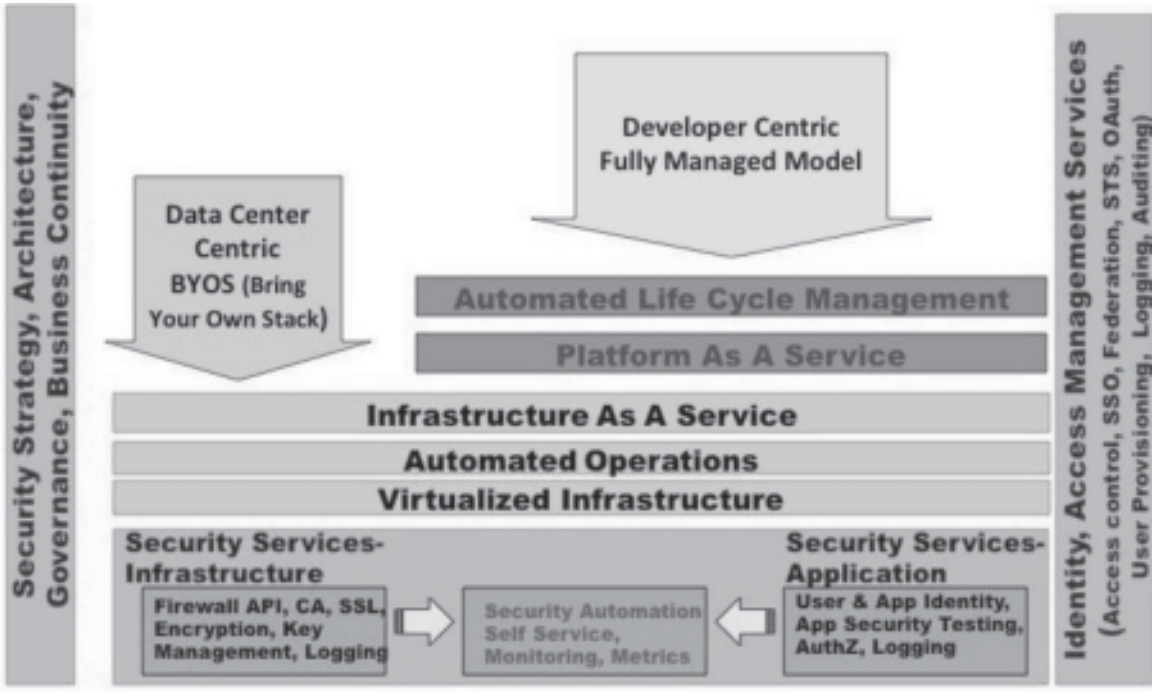

Fig. 4. Security Architecture for Cloud Service Layers

(*c*) Security Issues in IAAS

The Infrastructure as a Service layer provides the user with the operating area where he can have full control over the application that resides in the server. The security issues can be listed as follows:

1. Authentication and Authorization.
2. Denial of service attacks.
3. Cryptographic attacks, etc…

3. Threats and challenges in cloud computing layers

The root for most of the security problems arises from :

1. Loss of Control.
2. Loss of Trust.
3. Multi-tenancy.

These challenges can be manipulated and their deficiencies can be overcome with the following aspects;

1. **Loss of Control :** These are the following scenarios when the consumer has the possibility of losing their credentials and data;

   The applications that are controlled by the users that are held in space of any cloud service providers will have the data of an application as well as certain functionalities and resources are stored with provider. Another cause is that User Identity management and the security policies are handled by cloud provider (Nelson Gonzalez et al). To overcome these problems, the provider should take care of the privacy and legal agreements, monitoring all the repairs and requirements. The loss of control can be repaired by monitoring, utilizing multiple clouds, maintaining good control over access methodologies and authorization.

2. **Lack of Trust :** These SLAs typically state the high level policies of the provider (*e.g*. Will maintain uptime of 98%) and do not allow cloud consumers to dictate their requirements to the provider. Standard language must be used for the user understanding (Guoyuan Lin et al). As an instance user can given the idea or functionalities of a particular product, so that it will be helpful for the future users. The lack of trust can be minimized by the policy languages in human understandable formats and certification of trust explicitly showing its feedback.
3. **Multi-tenancy :** Since the cloud allows and gives permission for the users to access the shared pool of resources. So, there occurs the problem with the collaboration of multiple users accessing the same content. For example, if the consumer's policy requires isolation of VMs, the provider can construct an affirmation that says it uses cache partition to maintain VM isolation.

2. RESULTS AND DISCUSSION

There are various models that are designed and proposed by the researchers to overcome the security inefficiency of cloud layers and models.

When the user uploads the data in cloud, it will be stored anywhere in the cloud environment. Cloud storage is the upcoming feature that is been encouraged in current scenario, mechanisms has to be developed to overcome these faulty procedures. The proposed model gives a new adoption of an idea to protect the data in a well-organized way. The reformation of this model depicts that, when the owner of the data wants to upload a particular set of documents which usually contain the data and logic or he can uploads certain information with the help of search index to query and analyze the desired set of data, where in both the cases the data that has to be sent into the cloud server, where it will be encrypted with any cryptographic techniques(Jiadi Yu et al). On the course of encryption, public and private keys will be generated for the users' purpose, which can be used while retrieving the data from the server.

As the next pace, the encrypted data enters the server. Normally, all the cloud service providers like Amazon, Salesforce, and many other CSPs will have *n* number of servers employed for serving the purpose of secure storage of confidential data. The details are illustrated in Figure 5 shown below;

Fig. 5. Proposed Security Model for Cloud Data Upload.

Once the data is circulated to the respective space, it gets distributed among various servers located in the environment. And when the user wishes to retrieve the data, he can make a query to the cloud server through proper authentication methodology. Fig 5 elucidate the cloud servers on identification of the exact customer, it accepts the search query that has been put forward by the client or user. In response, One Time Password (OTP) will be generated in return to the user, so the user can request for the particular data and it will be decrypted with the cryptographic techniques using the private and public key, after all these standards of protection, the user can have access to the information securely.

1. Constructive Optimization of Security Performances and Parameters

On the onset of these security techniques, performance plays a vital role in maintaining efficient access of data, the various performance measures of protecting the data is been explained below;

Security Parameters Evaluating Performances

Input : Data, Data Protection, Data[ ]

Data [ ] array consisting of confidentiality, Integrity, Availability.

Output : Secure data from cloud service provider

Data owner to Service Requester

Begin

For $i = 0$ to n

$\text{Conf}[i] =$ Confidentiality;

$\text{Int}[i] =$ Integrity;

$A[i] =$ Availability;

$SD \text{ (Secure Data)} = \text{Conf}[i] \;\&\&\; \text{Security} \;\alpha\; \text{Int}[i] \;\&\&\; A[i]$;

$\text{Int}[i] \;\&\&\; A[i] = 1 / \text{Security}$;

Secure Data (SD) = True (achieved);

End;

The categorization of performance measures are explained below :

1. **Confidentiality :** It means that not providing unnecessary access rights to the unauthorized users or consumers. Loss of confidentiality can occur when an irrelevant action is been carried for using the particular data (Kevin Hamlen et al). This is possible only when the data that is uploaded in cloud is has not properly protected with encryption technology.
2. **Integrity :** Integrity is not assured when the data starts losing its original representation. When a hacker intrudes the system, he protrudes the required data by modifying its content or altering the whole content of the uploaded user data (Yan Zhu et al). This can be eliminated by proper cryptographic techniques which are done by encrypting the logic and data before reaching the storage provided by the cloud service provider.
3. **Availability :** The concept of availability is functionally an advantage as well as a drawback. Providing the access rights to all the users to manipulate the shared pool of resources.

3. CONCLUSION

Even though the concept of cloud computing has created hype among all categories of users and reached an unimaginable height in delivery of services as well as customization, still the problems in security remains. These scenarios pulled up all the IT industrialists and researchers to tranquil down the security problems. We can conclude from the above discussion that, the proposed security modelcan provided efficient protection for the user data with logics, algorithms, and cryptographic techniques. In addition to that, the trust and the legacy functionalities can be maintained without any security leakages. As a future enhancement, more powerful encryption and decryption techniques can be inculcated to handle the bigger data environments in cloud.

4. REFERENCES

1. Gkatzikis, L.; Koutsopoulos, I, (2013) "Migrate or not? exploiting dynamic task migration in mobile cloud computing systems," Wireless Communications, IEEE, vol.20, no.3, pp.24,32.
2. Guoyuan Lin; Danru Wang; YuyuBie; Min Lei, (2014) "MTBAC: A mutual trust based access control model in Cloud computing," Communications, China, vol.11, no.4, pp.154, 162.
3. Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Ninja Marnau, (2013) "Security and Privacy-Enhancing Multicloud Architectures", *IEEE Transactions On Dependable And Secure Computing*, VOL. 10, NO. 4.
4. Jiawei Yuan; Shucheng Yu, (2014) "Privacy Preserving Back-Propagation Neural Network Learning Made Practical with Cloud Computing," Parallel and Distributed Systems, IEEE Transactions in vol.25, no.1, pp.212, 221.

5. Jiadi Yu, Peng Lu, Yanmin Zhu, GuangtaoXue, and Minglu Li, (2013) "Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data", *IEEE Transactions On Dependable And Secure Computing*, VOL. 10, NO. 4.

6. Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, BhavaniThuraisingham, (2010) "Security Issues forCloud Computing",*International Journal of Information Security and Privacy*, 4(2), 39-51.7)

7. Khan, AR.; Othman, M.; Madani, S.A; Khan, S.U., (2014) "A Survey of Mobile Cloud Computing Application Models," Communications Surveys & Tutorials, IEEE, vol.16, no.1, pp.393, 413.

8 Nelson Gonzalez, Charles Miers, Fernando Red´ýgolo, Marcos Simpl´ýcio, TerezaCarvalho,Mats N¨aslund and MakanPourzandi, (2012) " A quantitative analysis of current securityconcerns and solutions for cloud computing", *Journal of Cloud Computing: Advances, Systems and Applications*.

9. QiangDuan; Yuhong Yan; Vasilakos, AV., (2012) "A Survey on Service-Oriented Network Virtualization Toward Convergence of Networking and Cloud Computing," Network and Service Management, IEEE Transactions on , vol.9, no.4, pp.373, 392.

10. SoaresBoaventura, R.; Yamanaka, K.; Prado Oliveira, G., (2014) "Performance Analysis of Algorithms for Virtualized Environments on Cloud Computing," Latin America Transactions, IEEE (Revista IEEE America Latina) , vol.12, no.4, pp.792,797.

11. Yan Zhu, Hongxin Hu, Gail-JoonAhn, Stephen S. Yau, (2012) "Efficient audit service outsourcing for data integrity in clouds", *The Journal of Systems and Software 85* 1083– 1095.