International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Cloud Computing Security

Arun Srinivas .R[1], Udhaya Kumar .V[2]

[1]MCA student (Computer Application), Department of Computer Applications, Prist Deemed to be University, Puducheery Campus, India

[2]Assistant Professor, Department of Computer Applications, Prist Deemed to be University, Puducherry Campus, India

Abstract: ***Cloud computing is a technology developed recently and being used for personal but also business purposes. Cloud security was vulnerable to threats and many cases had as result data loss, hacking, denial of services and etc but new security models and security tools are being improved. The purpose of this research is to define "cloud computing", its functionality and implementation, define the function of a cloud security and refer to its existence, a literature review for previews attempts and improvements, a research on open- source security tools, the implementation of a cloud server and demonstration of security protection on cloud servers. Sequence diagrams, use cases will be included for the explanation of the functionality and their interaction with the system, and for business environments a chapter will be included for the management of the physical teams.***

1. Introduction

As the world of technology and informatics is rising and new ambitions are gained, the more recent topics students choose the more knowledge they consolidate for their future development. Cloud Computing is a modern word and often used for something "new". It is also said that is destined only to group of experts. The meaning of cloud and its functionality had always existed since the application of the internet took place. Researchers and network engineers gave this technology the name "cloud" similar to the functions that physical clouds have. Cloud technology and networking since its implementation has been used for personal, academic but also business purposes, even famous consortium take advantage from it or even sell its services. What is cloud? Why made its appearance? What is its function to the real world? The introduction chapter will include these answers and will clear up all the mist in order to explain it in plain terms.

Figure 1: Cloud computing

1.1Services Models

Three types of cloud services and user can use any services which are mentioned below:

- Software as a Service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)

Software as a Service (SaaS): Provides applications from the infrastructure of the cloud and implements them on the end-user machine (sales force CRM, Gmail/Google Apps, Microsoft Live and etc).

Platform as a Service (PaaS): Provides platform, business and service tools, adds development and programming applications to Iaas, includes databases, web servers, execution frameworks/run-times and development tools.

Infrastructure as a Service (IaaS): It delivers computation, network resources, also includes servers, virtual machines, storage, load balance-rs and other core infrastructure stack.

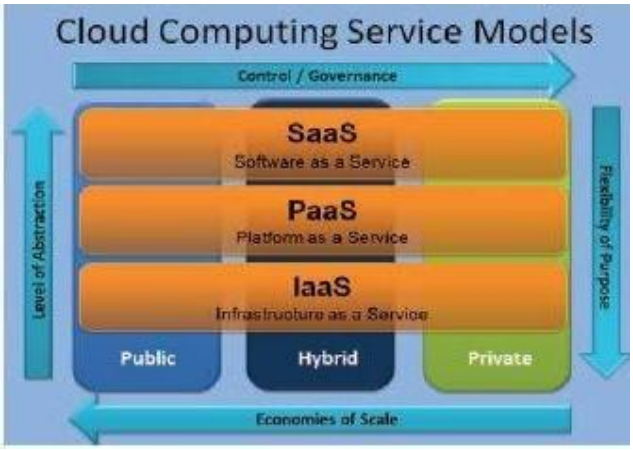

Figure 2: Illustrating the Cloud Computing Service Models

1.2 Deployment models

There are three Deployment Models and are described below:

Public Model Private Model Hybrid Model

Public Model: Designated for public clients that can register for a low price or even free and take advantage of the infrastructure (storage of data, software and etc). This infrastructure is available to the general public. As the name suggests, public cloud is a model in which resources are

generally available to everyone or anywhere.

Private Model: A cloud platform with dedicated use for home users or special organizations. This model is developed for the private organizations like one house and an organization and they can use it for their own purpose. This kind of a service is not accessed by everyone.

Hybrid Model: A private cloud that can expand to manage resources of public clouds. Hybrid Clouds are combination of public and private cloud in a same network. This can be done if private cloud need some important services from the public cloud like Private cloud can store some information on their private cloud and we can use that information on public cloud. In cloud computing, there are many issues but security is the major issue which we will discuss further.

2. Problem Statement

Our research focus on the security issues of data over a cloud. We will broadly cover the aspect of multi- tenancy in cloud computing which will meet the challenges of security of data, so that the data will remain protected while being on the network.

3. Literature Review

Arijit Ukil, Debasish Jana and Ajanta De Sarkar: In this paper, the problem of security in cloud computing has been analyzed. This paper gives security architecture and necessary support techniques for making our cloud computing infrastructure secured.

,

Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy: All the Security issues of cloud computing are highlighted in this paper, because of the complexity which users found in the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be changed or improved.

Kashif Munir and Prof Dr. Sellapan Palaniappan: In this study, we reviewed the literature for security challenges in cloud computing and proposed a security model and framework to make cloud computing environment secure.

Ayesha Malik and Muhammad Mohsin Nazir: In this paper, various techniques have been discussed which helps to protect the data, secure data such as:

- **Mirage Image Management System**: This system addresses the problems related to safe management of the virtual machine images that summarize each application of the cloud.
- **Client Based Privacy Manager**: This technique helps to reduce the loss of private data and threat of data leakage that processed in the cloud, as well as provides additional privacy related benefits.
- **Transparent Cloud Protection System (TCPS)**: This provides protection system for clouds designed at clearly monitoring the reliability of cloud components. TCPS is planned to protect the integrity of distributed computing by allowing the cloud to monitor infrastructure components.
- **Secure and Efficient Access to Outsourced Data**: This Provides secure and efficient access to Outsourced data is an important factor of cloud computing and forms the foundation for information Management and other Operations.

Krešimir Popović, Željko Hocenski: In this paper, security in cloud computing was discussed in a manner that covers security issues and challenges, security principles and security management models.

Takeshi Takahashi, Gregory Blancy, Youki Kadobayashiy, Doudou Fally, Hiroaki Hazeyamay, and Shin'ichiro Matsuo: This paper introduced technical layers and categories, with which it recognized and structured security challenges and approaches of multitenant cloud computing.

Nagarjuna, C.C kalyan srinivas, S.Sajida,lokesh: In this paper the main issue with multi tenancy is that the clients use the same computer hardware to share and process information and the result is that tenants may share hardware on which their virtual machines or server runs, or they may share database tables.

4. Existing Security Threats in Cloud Computing

Within a cloud environment we define as secure policy issues like "privacy, security, anonymity telecommunications capacity, government surveillance, reliability and liability". There is a difference between each type of client a cloud server deals with. Academia clients require more performance than security protection in comparison with business clients that want their data to be protected more than having use on a high performance system. Gartner's seven security concerns will be described below.

- Privileged user access.
- Regulatory compliance.
- Data location.
- Data segregation.
- Recovery.
- Investigate support.
- Long-term viability.

Privileged user access: Fragile data that can be analyzed from outsiders and give them ability of passing the "physical-logical" layer of the cloud and gain access on data and software.

Regulatory compliance: Clients are responsible for the good management and security of their data even in a cloud environment. Most cases show the percentage of data loss or privacy intrusion is caused from human factors that were clients.

Data location: Te exact location of the data clients uploaded is known by them, and the distributed data storage because of its behavior can lead to loss of control and it is good for customers to know where their data is stored before proceeding to the cloud.

Data segregation: Encryption and decryption of data in the cloud is essential but it cannot be the only way of solution as it is variable to attacks.

Recovery: In a case of server failure or denial of service how will the data of clients been restored? Does the cloud vendor have a backup plan of reverse engineer and protection of data? Are cloud managers capable of restoring data they have to be supported from an outsider third party company? These actions are not on client favor.

Investigate support: Cloud services are hard to investigate cause of many customers data placed in the same location, but can also spread infected files to other sets of software

Long-term viability: Cloud providers have to assure their clients that even in a case of a merge in a bigger cloud company there will still be integrity and availability on their data.

5. Existing Security Solutions

There are several solutions that exist in the internet environment that can run also to cloud infrastructures effectively but more cloud specified attacks need more expertise solutions. Internet solutions can be used to cloud systems or even improved.

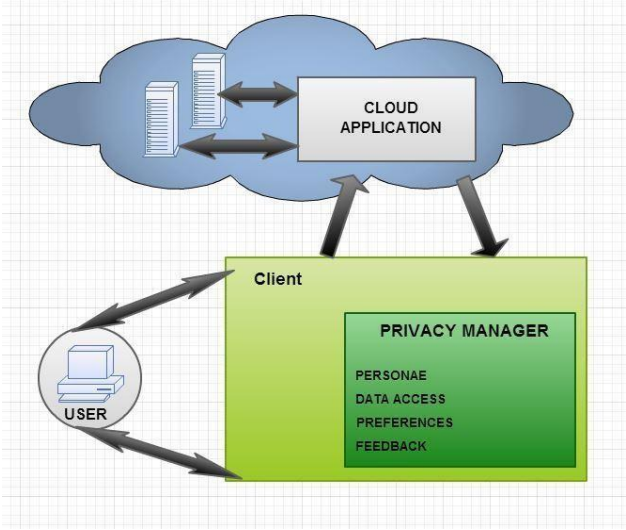

Figure 3: Proposed Solution

A. Access Control

The mechanisms of access control are tools that enable user authorized access and support the prevention of unauthorized ones to the infrastructure. These mechanisms should analyze users life-cycle by the time they sign up until their de-registration, so it would be sure they had no longer access. Special analysis should be put on user entering privilege mode and can modify system policies. The following steps should be considered to ensure security:

1) Control access to information.
2) Manage user access rights.
3) Encourage good access practices.
4) Control access to network services.
5) Control access to operating systems.
6) Control access to applications and systems.

In the SaaS model cloud provider is the one responsible for the management of the whole infrastructure. Application is delivered as a service to clients via a web browser so other network controls lose their power and get ignored by the user access controls. Clients should focus to their user access commands. In the PaaS model, cloud provider focuses on the management of access control to servers, network and application infrastructure.IaaS clients are responsible for every management aspect exists in this architecture. Access on virtual machines, storage, servers, and network should me designed to be managed from the clients.

B. Countermeasure and fast response

Common point in IT and cloud security of networks is investigation of possible problems and threats that can enter the system but more important is the implementation of the special response every problem needs to get. Cloud is set up on a group of specialized storage devices, lead by a custom high distribution coordinator, being available 24/7. For flexibility, scalability and efficiency usage of resources, cloud vendors must produce many solutions to almost any problems they face, in areas with great adaptability and workload analysis.

1) Partitioning

Workloads that have to come across multiple nodes, partitioning on data must occur in order to maximize transaction and better performance. The main goal is to minimize the chances of entering transactions to multiple nodes and result with the answer.

2) Migration

A cloud's main objective is the ability to have flexibility. In the "cloudpedia" this means concentrating more resources on components they need. There is a challenge on database programs that large amounts of data have to be transferred properly to other locations. In migration, the method works like predicting the adaptation time for example like partitioning time and breaking data into smaller parts in order to maintain transactions and simultaneously moving them.

3) Workload Analysis and Allocation

For better collaboration between virtual machines and their workloads, it is essential that analysis and classification is done to the resources required in order to estimate the virtual machine allocation memory.

C. Trace of user's behavior

Since most of the problems appear due to user novice knowledge on clouds and mistakes, method of tracing the user's identity and origin has already been implemented. Every cloud vendor knows users unique identity and can easily investigate on his behaviors. In order to maximize security, user's behavior has to be monitored from underground programs for criminal actions. Every suspicious move will be traced and will warn user or even ban according to the level of the act. In fact, those kinds of monitors have been used in IT environments such as TCP protocols for many decades. A good start would be to implement them also on cloud servers.

6. Future Work

The aim of this project is to theoretically explain the definition of the cloud, step by step appropriation of the reader on such terms and learning to keep a scope of security. In future work, we could design a framework which could satisfy the security issues related to multi-tenancy.

7. Conclusion

In conclusion, cloud computing is recently new technological development that has the potential to have a great impact on the world. It has many benefits that it provides to it users and businesses. For example, some of the benefits that it provides to businesses is that it reduces operating cost by spending less on maintenance and software upgrades and focus more on the businesses itself. But there are other challenges the cloud computing must overcome. People are very skeptical about whether their data is secure and private. There are no standards or regulations worldwide provided data through cloud computing. Europe has data protection laws but the US, being one of the most technological advance nation, does not have any data protection laws. Users also worry about who can disclose their data and have ownership of their data. But once, there are standards and regulation worldwide, cloud computing will revolutionize the future.

References

[1] Fusenig, V., Sharma, A., 2012. Security architecture for cloud networking, in: 2012 International Conference on Computing, Networking and Communications (ICNC). Presented at the 2012 International Conference on Computing, Networking and Communications (ICNC), pp. 45–49.
[2] Kandukuri, B.R., Paturi, V.R., Rakshit, A., 2009. Cloud Security Issues, in: IEEE International Conference on Services Computing, 009. SCC '09. Presented at the IEEE International Conference on Services Computing, 2009. SCC '09,
[3] Qaisar, E.J., 2012. Introduction to cloud computing for developers: Key concepts, the players and their offerings, in: Information Technology Professional Conference (TCF Pro IT), 2012 IEEE TCF. Presented at the Information Technology Professional Conference (TCF Pro IT), 2012 IEEE TCF.
[4] Ramgovind, S., Eloff, M.M., Smith, E., 2010. The management of security in Cloud computing, in: Information Security for South Africa (ISSA), 2010. Presented at the Information Security for South Africa (ISSA), 2010, pp. 1 –7.
[5] Shaikh, F.B., Haider, S., 2011. Security threats in cloud computing, in: Internet Technology and Secured Transactions (ICITST), 2011 International Conference For. Presented at the Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, pp. 214 – 219.
[6] Srivastava, P., Singh, S., Pinto, A.A., Verma, S., Chaurasiya, V.K., Gupta, R., 2011. An architecture based on proactive model for security in cloud computing, in: 2011 International Conference on Recent Trends in Information Technology (ICRTIT). Presented at the 2011 International Conference on Recent Trends in Information Technology (ICRTIT), pp. 661 –666.
[7] Tianfield, H., 2011. Cloud computing architectures, in: 2011 IEEE International Conference on Systems, Man, and Cybernetics (SMC). Presented at the 2011 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 1394 – 1399.