Cloud OS and Security Protocols

Mr. S. Gopalakrishnan[1], Ms. V. Sujitha[2]

Assistant Professor, Dept. Computer Applications, Pioneer College of Arts & Science, Coimbatore, Tamilnadu[1]

Student, Dept. Computer Applications, Pioneer College of Arts & Science, Coimbatore, Tamilnadu[2]

Abstract: In the current trends of computing, cloud computing plays a vital role and it is emerging at the level of maximum. The reason behind this is people started moving their data to cloud with the expectation of hundred percentage availability on their demand, i.e., anytime anywhere computing. Though the cloud services are provided by the third party, security becomes a very big question mark. The main objective of this paper is to provide an overview of cloud computing and its security, which help the young researchers to get clear idea.

Keywords: Computing, Cloud, Grid, Public, Private, Hybrid, IaaS, PaaS, SaaS, Security

I. INTRODUCTION

A new fashion of computing got and getting raised with the facility of dynamic scaling and offering the resources virtually as a service through the internet, called as cloud computing. Like other areas in the field of computer science, cloud computing also doesn't have a standard definition. US National Institute of Standards and Technology (NIST) gave a definition that covers all the aspects of cloud computing, that is "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. It made to trend like it is a mandatory computing for the users which will remold the information technology operations and the marketplaces.

The cloud computing has another name of "anytime-anywhere computing", i.e., the users of this computing are not dependent on a particular devices/nodes like the Personal Computers (PC), Laptops, Smartphone's, etc., and also they are not dependent on the timing. The main benefit of using this advanced computing is cost saving, high availability, and easy scalability. Figure 1, shows how the cloud computing got developed stage by stage from the mainframe computing.

In Mainframe computing, multiple users shared the great and powerful mainframes through dummy terminal. In PC Computing, personal computers are made powerful to face the user need in majority. In network computing, personal computers, laptops and servers were linked through local networks to share the data and also to increase the performance. In Internet computing, to form a global network local networks were connected to other local networks to use the remote applications and resources. In Grid computing, the computing power and memories are shared through a distributed computing system. In cloud computing, the resources are shared on the internet in a scalable, easy, effortless way.

The term cloud computing is a symbol for the internet. While the user draws any network diagrams the user use cloud symbol to denote the internet where it hides the compromising technology and the fundamental infrastructure. Cloud computing utilizes the internet to provide the computing services which include hardware, software, environments for testing, programming, etc., but the user don't know what the infrastructure is and where it is from.
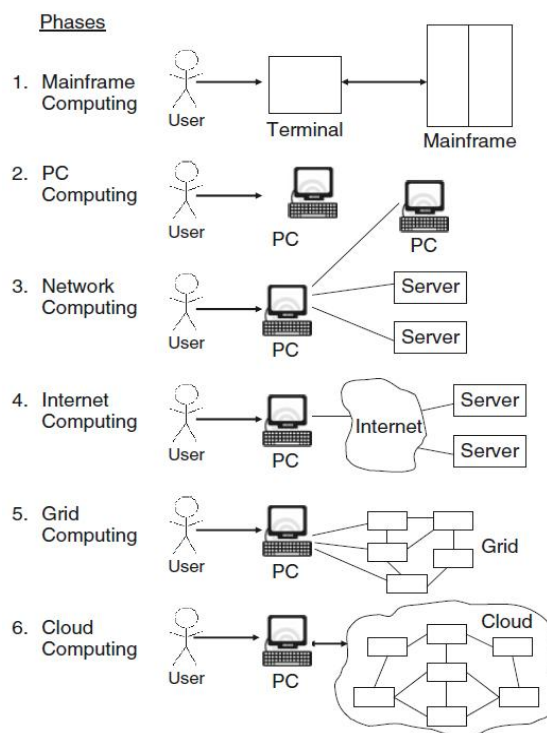

Fig.1: Mainframe to Cloud [Voas.J and Zhang.J.,2009]

II. CLOUD TYPES

There exists no condition or restriction that all users must use the same cloud for all their needs. Because different users have different needs. To meet the user's specific needs different types of cloud are available. The basic concept of computing is store and forward, which is provided by all the clouds. The cloud can be classified as Public Clouds, Private Clouds, Hybrid Clouds and Community Clouds.

2.1 Public Cloud

The most common cloud is public cloud where services are made available to the public. The public cloud can be sometime called as external cloud. The people can use this public cloud in a pay-as-you-go manner through the internet. Most enterprises have subscribed or consent the public clouds offered by the top companies named Google, Amazon and Microsoft. Even though the user use the top companies for their cloud services, still the question arise is "security", because the user are saving their data in a third party computer. They have chance to view or misuse the confidential data of the users.

2.2 Private Cloud

The private clouds are operated exclusively for business or organization. Mostly private clouds are used by the large companies or governments who want to keep their data in a well secured and controlled manner. The private cloud provides the guaranteed performance to meet the user needs. One of the disadvantage of private cloud is, it need more investment and need an expertise to manage.

2.3 Hybrid Cloud

Public cloud and private cloud combines to give hybrid cloud. To meet the specific needs user may need to use both public cloud and private cloud. By this cloud the user handle some of the resources internally and some other externally [BorkoFurhtand Armando Escalante.,2009].

2.4 Community Cloud

The main intention and infrastructure of this cloud was designed for specific community of users in organizations. It was mainly designed for the organization who jointly works with other organizations in the same environment.

III. TYPES OF SERVICE IN CLOUD

3.1 Software as a Service (SaaS)

It is the model where an application is hosted as a service in internet and the user can access it on the basis of pay for what you use. Some of the examples are Web content management, Video conferencing, Customer resource management (CRM).
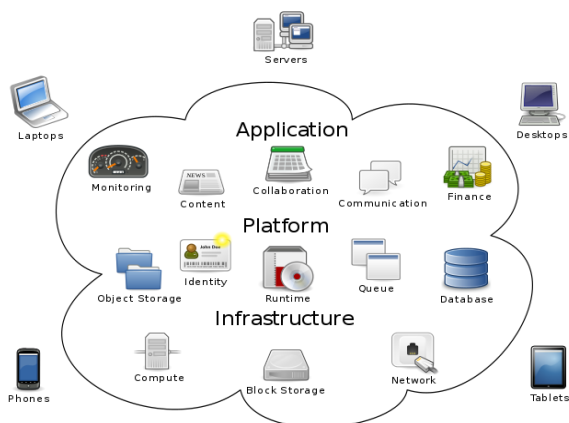

Fig.2: Elements of Services in Cloud

3.2 Infrastructure as a Service (IaaS)

It is the delivery of computer/server/network infrastructure through a environment called virtualization. User instead of buying software, hardware, server, equipments of network, they can simply use them like rent on the basis of pay for what you used manner. Due to this service, user will get saved a lot and lot of money.

3.3 Platform as a Service (PaaS)

This service incorporates the programming languages, tools and application delivery platforms are hosted by the provider of service to affirm development and delivery of end-user applications. Among all the services developer-oriented services is PaaS only. Integrated Development Environment (IDE) is provided by PaaS which incorporates data security, backup and recovery, application hosting, and scalable architecture.

IV. FAMILIAR THREATS IN CLOUD COMPUTING

In the daily life, like the cloud computing the threats in cloud computing also getting increased equally, the most familiar threats in cloud computing are [PatilMadhubala R,2015]:

- ✓ **Eavesdropping:** Deep enhanced spying of expected data, analysis of making congestion, discovering the data through the received loophole, plunging the trash data, checking or tracing the keystroke, sniffing of data packets were the category of eavesdropping to accumulate or observe the data.
- ✓ **Scam:** Making fraud, controlling the others data, exchange of misinterpreted data, destroying the integrity of data, change of data are the cases of misrepresentation.
- ✓ **Breaking-in:** Stealing of equipment (i.e., hardware) or programming (i.e., software) to find the private data for advantage.
- ✓ Destruction: In case of taking revenge this method is used, which is destroying the data, acknowledgements, etc
- ✓ **External attack:** Inserting the malicious code to monitor and gather the secret data.

V. ISSUES IN CLOUD COMPUTING

Issues in the cloud are endless and it gets increased periodically.This section discusses about the most common issues [K. Gandhi and P. Gandhi,.,2016] in cloud.

- ✓ **Legal Issues:** Users of the cloud trust the service providers and save their valuable data in the cloud. Day by day cloud storage levels gets increased up to the level which is not expected, the default question is "how safe it is?"
- ✓ **Privacy:** While the user uploads the data to the cloud, it is getting scattered and store in multiple datacenters, i.e., in the different location, the default question is, "whether they lose their confidentiality?"

✓ **Reliability:** Users are very much reliable on the services provided by the cloud service providers. Sometimes or most of the times users may be accessing the same data, the default question is, "whether users get their whole data at any time without any delay?"

✓ **Open Standard:** Principles of the all cloud are open to the world it may put the user's data into risk; the default question is, "whether there exist risk to the data in the cloud?"

✓ **Compliance:** Opportunity of face-to-face communication of messages to the service providers when there exist complaints, the default question is, "where do the users go and find the service providers?"

✓ **Freedom:** Cloud Users may need to move from cloud-to-cloud to fulfill their needs, the default question is, "whether the users get freedom in moving from a cloud service provider to another?"

✓ **Location Issues:** Cloud users are unaware of the data center's location; the default question is, "whether the cloud users get at least a location of the partial data that they have stored in the cloud?"

✓ **Soft Issues:** Cloud computing is also a computer network, the same level of security should be applied in the cloud, the default question is, "whether all cloud receives the same intensity of security when it faces the security attacks?"

VI. MODERN SECURITY PROTOCOLS IN CLOUD COMPUTING

G. Murali and R. S. Prasad.,2016 propose a strategy namely CloudQKDP (Quantum Key Distribution Protocol for Cloud Computing) which accomplished the advantages of mechanism using quantum mechanisms to secure cloud storage and data dynamics. Identity [ID] Management is considered as an headache in cloud computing. I. S. Stop et al.,2013 proposed enhanced Identity Management Protocol [IDM3G] to deal the administration of cloud user and the security issues which arise because of the ID.

To reduce the issue related to trust management U. A. Kashif et al., 2015 proposed Distributed Trust Protocol for Infrastructure as a Service (IaaS) in Cloud Computing between cloud customer and supplier. To utilize and exchange the information in different cloud and grid environment R. Rajagopal and M. Chitra.,2012 proposed an IS (Interoperability Security) protocol.After examining the three protocols SAML (Security Assertion Markup Language), OAuth (Open Authentication) and OIDC (Open ID connectivity), N. Naik and P. Jenkins.,2016 proposed a prototype to investigate the cloud environment. Xiao Liu et al.,2012 have analyzed the schemes available for storing the data in cloud and propose SSOP (Secure Storage Outsourcing Protocols) which maintain the existing methods and overcome their security shortages.B. Feng et al.,2016 proposed a protocol based on the idea of auditing namely Privacy-Preserving-Auditing (PPA) protocol which plans and aims to support the dynamic data operations. Also it supports bidirectional authentication.

VII. CONCLUSION

Cloud computing becoming success for most users due to the services provided by the cloud service providers, but still many users face problems the reason behind this is they didn't understand the cloud computing fully. Researchers of Cloud computing society are working towards it to overcome it. This paper has provided an overview about cloud computing, types of cloud, different types of services, threats, issues and security protocols for cloud computing. We hope this paper would be a gateway for the young researchers to understand the cloud computing and propose a better protocol to overcome the security issues.

REFERENCES

[1] B. Feng, X. Ma, C. Guo, H. Shi, Z. Fu and T. Qiu, "An Efficient Protocol With Bidirectional Verification for Storage Security in Cloud Computing," in IEEE Access, vol. 4, no. , pp. 7899-7911, 2016.

[2] BorkoFurht, Armando Escalante, "Handbook of Cloud Computing", Springer, 2010.

[3] G. Murali and R. S. Prasad, "CloudQKDP: Quantum key distribution protocol for cloud computing," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-6.

[4] I. S. Park, Y. D. Lee and J. Jeong, "Improved Identity Management Protocol for Secure Mobile Cloud Computing," 2013 46th Hawaii International Conference on System Sciences, Wailea, HI, USA, 2013, pp. 4958-4965.

[5] K. Gandhi, P. Gandhi, "Cloud computing security issues: An analysis," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 3858-3861. H. Zhu, "Towards a Theory of Cloud Computing in the Protocol-Composition Framework," 2010 Third International Symposium on Intelligent Information Technology and Security Informatics, Jinggangshan, 2010, pp. 758-762.

[6] N. Naik and P. Jenkins, "An Analysis of Open Standard Identity Protocols in Cloud Computing Security Paradigm," 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/ CyberSciTech), Auckland, 2016, pp. 428-431.

[7] PatilMadhubala R., "Survey on security concerns in Cloud computing," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015, pp. 1458-1462.

[8] R. Rajagopal and M. Chitra, "Trust based interoperability security protocol for grid and Cloud computing," Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on, Coimbatore, 2012, pp. 1-5.

[9] U. A. Kashif, Z. A. Memon, A. R. Balouch and J. A. Chandio, "Distributed trust protocol for IaaS Cloud Computing," 2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, 2015, pp. 275-279.

[10] Voas.J, Zhang.J, "Cloud computing: New wine or just a new bottle?", IEEE ITPro, April 2009. Pp.15–17.