

Cloud Computing and Its Security Issues: Survey

Syeda Baseer Unnisa Begum,
Assistant Professor, Department of Computer Science (MCA), R. G. Kedia College of Commerce, Hyderabad,
Telangana State, India

Abstract— Cloud computing is emerged as an essential technology in IT field from past two decades. Cloud computing is a pay-per access technology in which computing services like storage, infrastructures, and application services are accessed by its users on paid basis over internet. Most of the enterprises and organizations are migrating their business to cloud because of its various characteristic advantages like reliability, scalability, agility, high performance efficiency and cost-effective nature when compared to having own IT infrastructures. Cloud also reduces the burden of cost and administration of IT infrastructure while companies can focus on their business prospects. Data over cloud can be affected by issues like integrity, security and unauthorized access by external users or attackers. Organizations are concerning about its security related issues while adapting its services. The objective of this paper is to give a review on the cloud computing and some of its security related issues.

Keywords— Cloud Computing, Cloud Computing Security, Cloud Deployment Models, Cloud Service Layers, Security Issues.

I. INTRODUCTION

In accordance with National Institute of Standards and Technology, Cloud computing is defined as offering uninterrupted access to shared resources like hardware and software services to its users via internet on pay-per-access basis. Further access to these resources can be accordingly extended or reduced to a limit as per its client's demand [23]. Cloud computing offers the capability of accessing shared resources and infrastructure services that are provided by Cloud Service Providers (CSPs) to their clients on-demand basis through internet which converge with client's business requirements [4]. The popularity and market of cloud computing is advancing at past pace because of its various advantageous factors like scalability, agility, business continuity, reliability and low cost. According CAGR report global cloud computing market share will increased to USD512.81 billion by 2022 which is USD103.35 billion in 2015, means it would see an upward growth of 25.7% by 2022. A typical architecture of cloud computing is shown below (Figure 1).

Fundamentally, cloud Computing servers as a three layer architecture they are IaaS (Infrastructure as a Service) layer, PaaS (Platform as a Service) layer, SaaS (Software as a Service) layer. In IaaS layer CSPs provides infrastructural services like hardware, and network infrastructures to their clients as per client's computing requirements. PaaS layer offers computing platforms like Operating Systems to its clients. SaaS layer provides fully developed software applications to cloud clients.

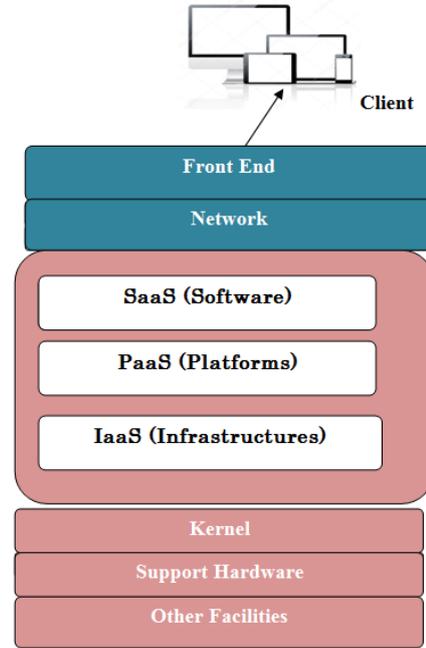


Figure 1. Cloud Computing Architecture

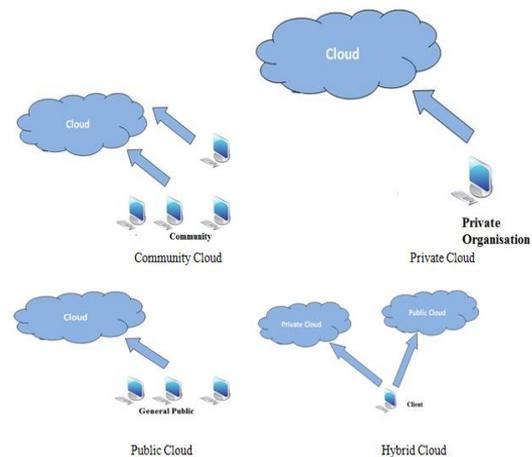


Figure 2. Cloud deployment Models.

Cloud computing serves in four deployment models (Figure 2), public, private, community and hybrid models. In public cloud, general public can access cloud resource services provided and maintained by a particular CSP. Some of public cloud providers are Amazon (AWS), Rackspace (Cloud Suite), and Microsoft (Azure Service), Google and Oracle Cloud Platforms. In Private Cloud, cloud services provided to a specific client organization within its boundary and resources are only accessed by the members of the same client organization, and not accessible by any other organization. Community cloud is combination of various kinds of clouds like private, and public, and is intended for group of users who are associated with different organizations or set of organizations for specific objectives. Community cloud can provide either on premise or off premise services. Hybrid

cloud is a mixture of two or more cloud models which possess unique framework that will have data and application mobility but are limited only to CSP and client by standardized technology. Since hybrid cloud is combination of public and private clouds it is more flexible and efficient than public cloud and private clouds alone and offers client enterprises to access non-core applications and core applications. Notwithstanding with its various advantageous and popularity, cloud has lack of security related worries, which are very crucial issues those needs to be solved [1]. Although cloud becoming, are popular than ever, most of organizations are still keeping distance from cloud services because of its security related issues. Security takes very crucial and significant role in success of cloud business. Cloud clients are does not want jeopardy situations by putting their crucial data and important applications over some others storage and needs their permission to access. Next section discusses some of security related issues to be concerned about cloud computing.

II. CLOUD COMPUTING SECURITY ISSUES

Cloud computing is a process of enlarging the capabilities of Hardware infrastructure, Software dynamically with no need of further investment. Anyhow, cloud computing has to bother about accessing software applications, data storage and processing power over internet all the time. Cloud computing has been progressed as a auspicious business technology to one of the fast growing domain of the IT industry. Yet more and more data of clients is placed on cloud, worries are increasing towards the safety of environment. Security has become major challenge and setback for adapting cloud computing. Once clients put their sensitive data over cloud they lost control of their data and they don't know what is happening with their data [11]. The important concern is how CSPs overcome issue of security [24]. Several security issues are emerged along with the advancement of cloud computing since it embraces various technologies compromising network infrastructure, database applications, operating systems, virtualization, resource and transaction management, load balancing, and memory management [8]. Below mentioned are some of the security issues related to cloud computing.

A. Lost Control of Data

Cloud computing is transforming the system of information management, specifically while processing client's personal data. Putting sensitive personal information of server located somewhere and administered by someone will have huge issue of privacy. Since cloud clients lost manual control over their data and applications placed on cloud that could become a major problem if cloud is exposed to attackers or when CSPs are compromised and share one's personal data with other unauthorized persons, and physical damage happens to cloud infrastructures.

B. Data Loss

When CSPs don't have proper data backup mechanisms or when data on cloud accessed by unauthorized users, actual clients data may be lost or stolen. This is will become a big issue for CSPs and Client organizations. Sometime employee of CSPs becomes turn against their company which they destroy the clients data or cause severe damage to CSP's security mechanisms which put both CSP and clients in jeopardy situation. CSPs must ensure the customer about the recruitment of employees and how they are providing access to resources and how they keep track of their activities. There is also a chance of natural disasters which

may cause severe data loss to CSPs as well as customer data. CSPs must have effective disaster recovery mechanisms to overcome these problems and to ensure safety for client's data.

C. Transparency

When CSPs does not reveal details about their internal policies, customers doesn't get knowledge about their data safety. CSPs must maintain transparency such as they must reveal about their data handling mechanisms, security polices in the cloud.

D. Unauthorized Access

Unauthorized access control will cause severe security issues like data theft and data destroying etc. CSPs must provide strong access contrail mechanisms for secure authentication, identification, and authorization of their users. Insecure web application interface leads the system to expose to unauthorized access. Additionally, lack of strong authentication technique may increase the chance of unauthorized access to data or resources. CSPs main responsibility is provide privacy of customer's data by posing strong authentication mechanisms.

E. Vendor Lock-in

To win the competition in market cloud vendors will place more than one deployment model layers. Here issue of vendor lock-in occurs since cloud platform uses tools and libraries that lock the application to the platform. Also the cost is high while client enterprises want to migrate from one platform to another application platform to take advantage of new services. Also sometimes cloud vendors do not provide services as per the client's demands. Some time issue rises with lack quality of services with existing infrastructures and unsure cloud resource provisions.

F. Account, Service and Traffic Hijacking

There are several new types of attacks happening that caused account, service and network traffic hijacking. Attacks like DoS, DDoS, man-in-the-middle attacks, and phishing, spam will cause problems in accessing of services, network.

G. Web Application Attacks

As stated by Verizon in its latest report web application attacks are increased by 300%. Attackers are using flaws in web interfaces to attack when cloud customer tries access the cloud resources through flawed web interface.

H. Cloud Misconfigurations

In recent most of cloud attacks are happened because of cloud misconfigurations. Problems arise with poorly configured or implemented security mechanisms allow data, applications and other resources to expose easily.

I. Visibility

One of the major contributors to recent security breaches is lack of visibility and vigilance. One should require to have well detailed visibility of data and resources over cloud and timely monitoring of network traffic is crucial thing if you want detect security breaches.

CONCLUSION

Since Popularity of cloud is advancing at great pace from past two decades, the chances of this technology could expose to security threats increasing. This paper presented some of security attacks that can cause critical issues cloud

computing environment. Most of security breaches are happened in recent past because lack of proper maintenance of security mechanisms, efficient monitoring and authentication mechanisms. Since safety of sensitive information is very important in this technology CSPs must have most advanced transparency security technique.

References

- [1] Archana Lisbon A, Kavitha R, "A Study On Cloud And Fog Computing Security Issues And Solutions", *Ijirae*, Volume 4, Issue 3, March 2017.
- [2] Manju Khari, Manoj Kumar And Vaishali, "Comprehensive Study Of Cloud Computing And Related Security Issues", *Advances In Intelligent Systems And Computing*, Big Data Analytics Proceedings Of Csi 2015.
- [3] G.Praveen Kumar, S.Kavitha, "A Survey On Security And Privacy Issues In Cloud Computing", *Ijirce*, Volume 5, Issue 7, July 2017.
- [4] Nirmal Kumar Gupta, "Addressing Cloud Computing Security Issues And Its Solution", *Ijst* Volume 8, Issue 4, Oct - Dec 2017.
- [5] G.L.Masala, P. Ruiu, A. Brunetti, O.Terzo, E. Grosso, "Biometric Authentication And Data Security In Cloud Computing", *International Conference On Security And Management*, 2015.
- [6] Md. Sakib Bin Alam, "Cloud Computing – Architecture, Platform And Security Issues: A Survey", *World Scientific News*, 2017.
- [7] Anand, "Cloud Computing And Cloud Related Security Issues", *Ijarc*, Volume 8, No. 5, May-June 2017.
- [8] Prince Kwame Senyo, Erasmus Addae, Richard Boateng, "Cloud Computing Research: A Review Of Research Themes, Frameworks, Methods And Future Research Directions", *International Journal Of Information Management*, 2018.
- [9] D.Sasikumar, S.Saravanakumar, "Cloud Computing – Research Issues, Challenges, Architecture, Platforms And Applications", *Ijltet*, Volume 5, Issue No 2, Mar-Apr 2017.
- [10] Khalil H. A. Al-Shqeerat, Faiz M. A. Al-Shrouf, Mohammad R. Hassan, Hassen Fajraoui, "Cloud Computing Security Challenges In Higher Educational Institutions - A Survey", *Ijca*, Volume 161, Issue No 6, March 2017.
- [11] Kuyoro S. O., Ibikunle F., And Awodele O., "Cloud Computing Security Issues And Challenges", *Ijcn*, Volume 3, Issue 5, 2011.
- [12] S. Hendry Leo Kanickam, Dr.L.Jayasimman, J.Iswarya, "Cloud Computing Security: Survey On Issues And Challenges", *Irjet*, Volume 05, Issue 02, Feb 2018.
- [13] Geeta C M, Et Al., "Data Auditing And Security In Cloud Computing: Issues, Challenges And Future Directions", *Ijc*, Volume 28, Issue No 1, 2018.
- [14] P. Ravi Kumar, P. Herbert Raj, P. Jelciana, "Exploring Data Security Issues And Solutions In Cloud Computing", *Icsec* 2017, December 2017
- [15] Dhaivat Dave, Et Al, "Cloud Security Issues And Challenges", *Advances In Intelligent Systems And Computing*, Big Data Analytics Proceedings Of Csi 2015.
- [16] Pooja Jayant, Nitesh Gupta, Umesh Lilhore, "Instruction Detection Over Over Cloud: A Survey", *Irjet*, Volume 05, Issue 02, Feb-2018.
- [17] Prof.(Dr.) Pradeep Kumar Sharma, Prof. (Dr.) Prem Shankar Kaushik, Prerna Agarwal, "Issues And Challenges Of Data Security In A Cloud Computing Environment", *Ieee*, 2017.
- [18] Teófilo Branco Jr., Filipe De Sá-Soares, Alfonso Lopez Rivero, "Key Issues For The Successful Adoption Of Cloud Computing", *Centeris*, November 2017.
- [19] Blesson Varghese, Rajkumar Buyya, "Next Generation Cloud Computing: New Trends And Research Directions", *Elsevier B.V.*, 2017.
- [20] Muhammad Faheem Mushtaq, Urooj Akram, Irfan Khan, Sundas Naqeeb Khan, Asim Shahzad, Arif Ullah, "Cloud Computing Environment And Security Challenges: A Review", *Ijacsa*, Volume 8, Issue No 10, 2017.
- [21] George A. Gravvanis, Et Al., "Recent Trends In Cloud Computing", *Special Issue, Future Generation Computer Systems*, 2018.
- [22] Madhumala R B, Dr. Harshavardhan Tiwari, "A Review On Cloud Computing Security Issues And Challenges", *Racsit-17*, Volume 5, Issue 4, April 2017.
- [23] Mohammad Ubaidullah Bokhari, Qahtan Makki, And Yahya Kord Tamandani, "A Survey On Cloud Computing", *Advances In Intelligent Systems And Computing*, Big Data Analytics Proceedings Of Csi 2015.
- [24] Arun Kumar Sen, Pradeep Kumar Tiwari, "Security Issues And Solutions In Cloud Computing", *Iosr-Jee*, Volume 19, Issue 2, Mar-April 2017.
- [25] Abdulaziz Alshammari, Sulaiman Alhaidari, Ali Alharbi, Mohamed Zohdy, "Security Threats And Challenges In Cloud Computing", *Ieee*, 4th International Conference On Cyber Security And Cloud Computing, 2017.
- [26] G Likitha Reddy And B. S. S. Murali Krishna, "Survey Of Cloud Computing And Its Application", *Ijasre*, Volume 4, Issue 1, January-2018.
- [27] Prof.Aruna P.Gurjar, Dr.Satyen M.Parikh, Dr.Jigneshkumar A.Chauhan, Prof.Jigarkumar D.Patel, "The Security Issues In Cloud Computing", *International Journal Of Advanced Research In Computer Science*, Volume 9, Issue No 1, January-February 2018.