A Survey on Cloud Computing Security Issues

Adarsh K Thampi
MPhil Scholar
Department of Computer Application
CMS College of Science and Commerce
Coimbatore, India
Email id: adarshkthampi@outlook.com

Dr.S.P Swornambiga
Associate Professor
Department of Computer Application
CMS Collge of Science and Commerce
Coimbatore, India
Email Id: swornagoms@gmail.com

Abstract— Cloud computing is the new technology advancement in the industry. It is the way to increase the capacity or capabilities dynamically without spending money for new infrastructure. As information exchange stands an important role in today's life, information security become more important. According to Forbes report in 2015, Cloud based security spending is expected to increase by 42%. International data corporation (IDC) in 2011 showed that 74.6% of enterprise customers ranked security as a major challenge. This research is to understand the cloud components, security issues and risks, along with the developing solutions that they actually mitigate the vulnerabilities in the cloud. However, the acuity with the cloud security needs improvement for the higher rate of adoption and need to solve as soon as possible.

Keywords— ***Cloud computing, Cloud Security, Security issues.***

I. Introduction

Cloud computing being adopted by wide range of users from commercial entities. According to right scale survey[1], across all users, AWS increased adoption from 57 percent in 2017 to 64 percent in 2018; Azure increased from 34 to 45 percent; Google Cloud increased from 15 to 18 percent; IBM could increase from 8 to 10 percent; VMWare Cloud on AWS came right out of the gate strongly with 8 percent adoption; Oracle Cloud increased from 3 to 6 percent and Alibaba Cloud showed 2 percent adoption. Cloud computing can be defined as a parallel and distributed computer system with a collection of interconnected resources based on service-level agreements (SLA)established through negotiation between the service provider and consumers. Adoption of cloud computing is reaching to maximum point and more companies are changing their old traditional workloads to cloud storage and services. There are many problems need to identify and analyze. In this article consolidates various works that address and risks, vulnerabilities in cloud computing. It also provides information about cloud architecture.

We can summarize the main features of cloud computing as follows:

- Cloud computing uses Internet technologies to offer scalable and elastic services; the term “elastic computing" refers to the ability to dynamically acquire computing resources and to support a variable workload.
- The resources used for these services can be metered and the users can be charged only for the resources they used.
- The maintenance and security are ensured by service providers.
- The service providers can operate more efficiently due to specialization and centralization.
- Cloud computing is cost-effective because of the multiplexing of resources; lower costs for the service provider are past to the cloud users.
- The application data is stored closer to the site where it is used in a device and location in independent manner; potentially, this data storage strategy increases reliability, as well as security and lowers communication costs.

A. Cloud Architecture

According to National Institute of Standards and Technology (NIST), “the cloud computing is a model for enabling convenient, resource pooling, ubiquitous, on-demand access with which can be easily delivered with different types of service provider interaction” [2]. Before we entering to security issues to the cloud computing security issues, it is important to understand cloud architecture.

According to NISTs Cloud Computing Reference Architecture, there are five major actors that are obstructed by cloud computing.

Table 1 Actors in NIST Cloud Computing Reference Architecture

Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, Cloud Providers
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from Providers to Cloud Consumers.

Table 1

B. About Cloud Computing

Cloud computing offers flexible, reasonable, and proven delivery platform for business and or IT Services over the Internet. In a cloud computing platform, the entire data transfers over a set of network resources, and it available through the virtual machines. The NIST Definition of Cloud Computing [3]

“Cloud Computing is a model for enable unlimited network access, conventional usage, on-demand service and scalable resources that are billed on utility basics”.[4] However cloud computing increases a level of risk because important services are outsourced to third party, which makes tougher to maintain privacy and data security. cloud computing supports various computing services that can be accessed by anywhere in the world. It can deploy, allocate or reallocate resources dynamically with ability to continuously monitor their performance [5]. cloud computing assigns five essential characteristics that cloud computing systems must offer

- **On-demand self-service:** A client can provision computer resources without the need for interaction with cloud service provider personnel.
- **Broad network access:** Access to resources in the cloud is available over the network using standard methods in a manner that provides platform-independent access to clients of all types. This includes a mixture of varied operating systems, and thick and thin platforms such as laptops, mobile phones, and PDA.
- **Resource pooling:** A cloud service provider creates resources that are pooled together in a system that supports multi-tenant usage. Physical and virtual systems are dynamically allocated or reallocated as needed. Fundamental in this concept of pooling is the idea of abstraction that hides the location of resources such as virtual machines, processing, memory, storage, and network bandwidth and connectivity.
- **Rapid elasticity:** Resources can be rapidly and elastically provisioned. The system can add resources by either scaling up systems (more powerful computers) or scaling out systems (more computers of the same kind), and scaling may be automatic or manual. From the perspective of the client, cloud computing resources should look limitless and can be purchased at any time and in any quantity.
- **Measured service:** The use of cloud system resources is measured, audited, and reported to the customer based on a metered system. A client can be charged based on a known metric such as amount of storage used, number of transactions, network I/O (Input/Output) or bandwidth, amount of processing power used, and so forth. A client is charged based on the level of services provided. While these five core features of cloud computing are on almost anybody’s list, the following are the additional advantages:
- **Lesser costs:** Because cloud networks operate at higher productivities and with greater utilization, significant cost drops are often encountered.
- **Ease of utilization:** Depending upon the type of service being offered, it is not requiring hardware or software licenses to implement service.
- **Quality of Service:** The Quality of Service (QoS) is something that can obtain under contract from vendor.
- **Reliability:** The scale of cloud computing networks and their ability to provide load balancing and failover makes them highly reliable, often much more reliable than in a single organization.
- **Outsourced IT management:** A cloud computing deployment lets someone else manage computing infrastructure while manage the business. In most instances, it can achieve considerable reductions in IT staffing costs.

C. Cloud Computing Service Models

The Three most common types of cloud service models [6] based on its capabilities and performances like infrastructure as a Service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS).

- Infrastructure as a Service (IaaS): IaaS deals with computer hardware (network storage, virtual server, machine, data center, processor, and memory) as a service.
- Platform as a Service (PaaS): It gives full access to developer to develop applications on a service provider platform. Fully Virtualized platform for one or more virtualized servers and specific applications.
- Software as a Service (SaaS): SaaS is a collection of remote computing services. It allows the applications to deploy remotely by third-party vendors.

D. Cloud Computing Deployment Models

The Cloud computing Deployment models describes about the purpose and nature of the cloud. NIST [2] defines five types of deployment models.

- Private Cloud: Resources are dedicated to a single or a set of organizations and treated a intranet functionality.
- Public Cloud: Resources are dynamically provisioned on a self-service basics.
- Hybrid Cloud: it functioned by the combination of one or more models.
- Community Cloud: its referred by a cloud infrastructure shared by several organization by within specific community.

II. VULNERABILITES OF CLOUD COMPUTING

A. Threats to cloud Computing

Cloud Computing is a combination of technology, process, people. There are many security issues for cloud computing and its process. According to Cloud Security Alliance [7] Fig 1 shows threats to cloud computing in all cloud computing environments [8]

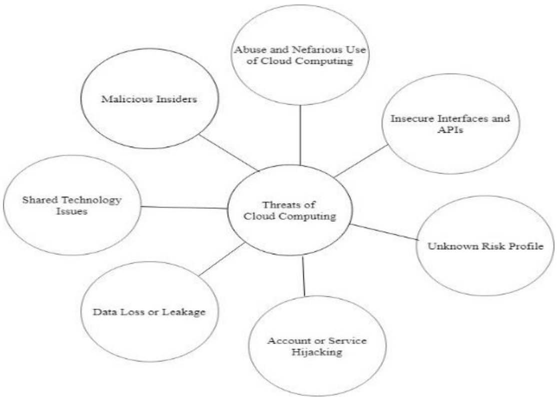
Abuse and Nefarious Use of Cloud Computing
Malicious Insiders
Insecure Interfaces and APIs
Shared Technology Issues
Threats of Cloud Computing
Unknown Risk Profile
Data Loss or Leakage
Account or Service Hijacking

Fig 1 Threats of Cloud Computing

- *Data Loss or Technology:* it is a very serious problem faced by cloud computing. If a provider may fraudulently retain additional copies of the data in order to share interested third parties.
- *Account or Service Hijacking:* vulnerable computer is replaced by the IP address for the credit of client and server will continue believe as a trusted client
- *Unknown Risk Profile:* Risk of compromised profile leads to loosing access to privileged account might mean loss of service.
- *Insecure Interfaces and API's:* Any vulnerability in cloud provider's API leads to significant risk or browser attack.
- *Abuse and Immoral Use of Cloud Computing:* In cloud computing registration process, anyone having a valid credit card can register and use the service. This facilitates anonymity, due to which spammer, malicious code authors and criminals can attack the system.
- *Malicious Insiders:* Malicious insiders' impact on organization is considerable. Given their level of access, they can infiltrate organizations and assets and do brand damage, financial losses and productivity losses
- *Shared Technology Issues:* Increased leverage of resources gives the attackers a single point of attack, which can cause disproportional to its importance.

III. SOLUTION FOR CLOUD COMPUTING SECURITY ISSUES

There are some cloud security solutions to adopt both service providers and the cloud consumers. Service Level Agreements (SLA) is the legal document between the customer and the service Provider. However, there are some best practices in countermeasures and controls that can be adopted. Security allows the confidentiality, integrity, authenticity and availability of information. The development of technologies and their standardization makes available a set of algorithms and protocols to counter cloud computing security issues.

A. Countermeasures for Cloud Computing security issues

The best and more important countermeasure for cloud computing security is

- *End-to-end encryption: The delivery of data can be secured by algorithms with top level encryption.*
- *Scanning for Vulnerabilities:* While the end-to-end encryption is implemented, highly recommended to scan unauthorized activities in cloud environment.
- *Authorization of Cloud Consumer:* cloud provider must be vigilant to take precautions to verify cloud consumer for preventing malicious attacks.
- *Secure Interfaces and API's:* An authentication gateway service (AGS) and an IAM system are implemented to identify and authenticate legitimate and grant them access, while denying access to intruders.
- *Image steganography:* it is a technique to cover information. So that the existence of the secret message cannot be detected easily.
- *DDoS Protection:* it is a technology to overcome multiple bot attacks from hackers. DDoS protection help to identify and prevent unauthorized multiple requests at a time.
- *Data Integrity Checks:* To ensure that data integrity is not compromised through deliberate or accidental modification, use resource permissions to limit the scope of users who can modify the data. Even with resource permissions, accidental deletion by a privileged user is still a threat (including a potential attack by a Trojan using the privileged user's credentials).
- *Network Security: N*etwork security is the key function to secure communication in cloud computing, network security concerns with both internal and external attacks. These attacks may happen in virtual or physical network.

IV. CONCLUSION AND FUTURE WORK

Security in cloud computing includes network security, component and control policies to organize secure data, applications and infrastructure that are connected with the cloud computing environment. Security issues in cloud computing is still difficult to sort out. This survey attempted to show various security challenges, vulnerabilities, attacks and threats that affect cloud computing. Unfortunately, there is no comprehensive solution for cloud security as for now, even the leading cloud providers such as Amazon, Google are facing security challenges and still searching for solutions.

For instance, every cloud computing environment faces various security vulnerabilities that could affect it badly and it could be prevented by adopting various security measures.

In cloud computing all users gain access to all application into data of all sorts, it also allows sharing or get shared information to the whole world or any group people in the cloud. cloud computing allows sharing of data on online level rather than using actual hardware or devices. A company offering secured cloud computing allows proper and secure sharing of information and cloud computing is not a product but a service offered by to cloud computing customers around the world to share or get shared data in a secured way.

References

[1] State of the Cloud Report. (2017). https://www.rightscale.com/lp/state-of-the-cloud

[2] National Institute of Standards and Technology

[3] Cloud Computing Implementation, Management and Security by John W. Rittnghouse and James F. Ransome

[4] Randeep kumar ,Jagroop Kaur(2015) Cloud Computing Security Issues and Its Solution: A Review(IEEE),978-9-3805-4416-8/15

[5] Thomas W. Shinder, ”Security Issues in cloud Deployment Models”, TechNet Articles,Wiki,Microsoft, Aug,2011. http://social.technet.microsoft.com/wiki/contents/articles/security-issues-in-cloud-deployment-models.aspx

[6] Kuyoro S.O., Ibikunle, F., and Awodele,.O.(2011). Cloud Computing Security Issues and solutions and Challenges. International Journal of Computer Networks (IJCN), Vol.3, Issue5, pp. 247-255

[7] Cloud Vulnerability incidents, 2013 Cloud Security Alliance, Ryan Ko, Stephen S G Lee.

[8] Essays, UK. (November 2013). Abuse And Nefarious Use Of Cloud Computing Information Technology Essay. Retrieved from https://www.uniassignment.com/essay-samples/information-technology/abuse-and-nefarious-use-of-cloud-computing-information-technology-essay.php?vref=1