ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management, Vol-4, Issue-4, 2020.

A Survey on Security Issues and Challenges in Cloud Computing

Md. Asadullah[1], Ritesh Kumar Yadav[2], Varsha Namdeo[3]

Department of Computer Science & Engineering[1,2,3]

SRK University, Bhopal, (M.P.), India[1,2,3]

ABSTRACT

In the computer's world these days cloud computing plays a very important role. It gives user facilities like a group of things such as software, platform, and infrastructure services. Virtualization is the backbone of cloud resource sharing. Security is also a main problem in the cloud. Multiple users have their perceptions related to the cloud. By using cloud computing, users can access resources anywhere by using the internet. So this technique is very useful in a user's daily life. One of the factors for cloud computing is cloud services which were provided by the cloud (IAAS, PAAS, and SAAS). These services enable users to access infrastructure, platform, and software. Even resources are allocated to users according to their requirements. But many people think it is unsafe to use cloud resources and its services. It is unsafe to use the cloud because there is no guarantee of information which is controlled or maintained by the vendors. Some security issues are noticed in cloud computing. In this paper, we have discussed a few issues with cloud computing and the challenges of cloud computing. This paper gives an overall investigation of security on data, protection, and issues in the cloud. The paper also defines the literature review related to cloud computing issues and threats and also the various security concerns are discussed.

Keywords: Cloud Computing, Security, Encryption, IAAS, PAAS, SAAS.

Introduction

The National Institute of Standards and Technology (NIST) has defined cloud computing as a technology that provides convenient access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) on-demand, which can be released with minimum management effort or service provider interaction and can also rapidly provisioned [1]. According to Google's Kevin Marks, the term cloud computing has evolved from the starting days of the Internet where the network was drawn as a cloud. The cloud hid the message from us, therefore we didn't care where the message was [2].

Based on user demands cloud computing also provide elastic resources with dynamic provisioning and scaling. This approach deals with the concepts of resource under-provisioning, i.e., fewer resources are allocated than needed and resource over-provisioning i.e., more resources are allocated than required. The elastic management increases system efficiency since it yields better overall system resource usage.

Cloud computing resources are managed by highly professional service providers which are provided in massive, abstraction (virtualization) based infrastructures, in contrast to the traditional computing model, where the computing power and the end-user data are located in the user's‟ local machines [3].

The cloud model increases the system reliability and efficiency while simplifying the installation, operation, and maintenance of information systems

and also reducing the costs. A cloud system requires less expertise to use therefore it is user friendly. We can co-relate the simplicity of the cloud usage with current running-water and electricity systems, where without being concerned with the technical complexity behind these systems; the end-users can easily use the services from providers. This paper highlights some areas for further work in cloud security, it also gives an overview of cloud computing and related security challenges.

II CLASSIFICATION OF CLOUD COMPUTING

Despite cloud computing being a relatively new and emerging term, most of the people believe that other forms of cloud used to exist even before this term was introduced. Though it is being referred by many names, other technologies and concepts are being developed and used to form the current cloud computing technology.

The abstraction of infrastructure complexities of data, applications, servers, and heterogeneous platforms where the infrastructure, servers, or applications can be used without knowing their exact location is the current brand of cloud computing (Cloud 3.0). Note that this internet development can also be plotted along other verticals, such as the semantic web, which among other things facilitates semantic search [4], which is not related to cloud computing directly, but can still be viewed as something that is enabled by the cloud computing paradigm [5]. The cloud-like structures are also being emerged in other fields such as process control systems and smart grid constellations [6]; the Advanced Metering Infrastructure brings the always-on aspect physically into people's homes. Eventually, a merger of all such domain-specific networks into a single global cloud is expected, as has long been a vision of telecom operators.

Cloud computing is classified based on either there:-

a. Deployment models
b. Service models.

Figure 1 shows cloud models based on the NIST definition framework [2]. The four widely referenced deployment models are private, public, community, and hybrid cloud.

1. Private Cloud: - The cloud infrastructure is operated within a single organization, and managed by the organization or a third party regardless of whether it is located premise or off-premise. The cloud resources are used by the organization itself for its private use. Private clouds are built by an organization for serving its critical business applications.
2. Public Cloud: - This type of cloud is the dominant form of the current cloud computing deployment model. The public cloud can be used by the general public cloud consumers for their benefits and the public cloud service provider has got the complete ownership of the public cloud with their policies, values, costing, and charging models. Many popular public cloud service providers are Amazon EC2, Force.com, Microsoft, and Google App Engine, etc.
3. Community Cloud: - This type of cloud is jointly constructed by certain organizations and the same cloud infrastructure as well as policies, requirements, values, and concerns is shared by them. Economic stability and democratic equilibrium are formed by the cloud community.
4. Hybrid Cloud: - This type of cloud infrastructure is a combination of two or more clouds, it can either be public, private, or community. The hybrid cloud is used by the organizations for optimizing their resources to increase their core competency by margining out peripheral business functions onto the cloud while controlling core activities on-premise through a private cloud.

The cloud service models are classified as Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Data Storage as a Service (DaaS).

1. Software as a Service (SaaS):- In cloud SaaS, the applications of the cloud consumers are released on a hosting environment that can be accessed from various clients (for e.g Web Browser, PDA, etc.) through a network by application users. Business applications like

Enterprise Resource Management (ERP), accounting, Customer Relationship Management (CRM) can be delivered by SaaS. Google Apps and Salesforce CRM are certain examples of SaaS. The underlying infrastructure is not controlled by consumers.

2. Platform as a Service (PaaS):- In cloud PaaS, the tools and resources on cloud infrastructure are used to provide services to the end-users. PaaS is a development platform with the help of which the cloud services and applications are directly developed by cloud consumers on the PaaS cloud. The examples of PaaS are Microsoft Windows Azure and Google App Engine. The underlying infrastructure and operating systems are not controlled by the consumers but the deployment of individual applications is controlled by consumers.

3. Infrastructure as a Service (IaaS):- In Cloud IaaS the fundamental computing resources such as storage, network, servers, etc. are used to provide services to the end-users. In IaaS cloud the concept of Virtualization is used extensively for integrating physical resources in an ad-hoc manner to meet the increasing and decreasing demand from cloud consumers. Amazon EC2 is an example of cloud IaaS. The underlying infrastructure is not controlled by the consumers but typically the virtual machines can be launched with a chosen operating system, which in turn is managed by the consumers.

4. Data Storage as a Service (DaaS):- The cloud DaaS can see as a special type of cloud IaaS in which on-demand delivery of virtualized storage has become a separate cloud service – data storage service. Amazon S3, Google BigTable are examples of cloud DaaS.

Many large organizations such as Google, Yahoo, Amazon, Facebook, etc are currently using cloud computing since it has many disadvantages. Since it saves a lot of initial investment cost therefore it is very beneficial for start-ups also. Some examples of start-ups are Dropbox and Groupon etc. which utilize cloud computing for their daily operations. Now to reduce investment and operation costs various other companies are also moving their applications to cloud for increasing their business efficiency.

III Security Issues In Cloud Computing

Various security threats must be taken into consideration for getting the full benefit from this new computing paradigm. Some of the security concerns are listed and discussed below:

1) Security concern 1: If the user decides to move from one cloud to the other cloud there can be the incompatibility issue with storage services provided by one cloud vendor with other cloud vendors services (e.g. Google cloud is incompatible with Microsoft cloud) [7].

2) Security concern 2: The data logs must be provided to security managers and regulators, in the case of Payment Card Industry Data Security Standard (PCI DSS). [8]

3) Security concern 3: The control of physical security is lost with the cloud model since computing resources are shared with other companies. There is no knowledge or control of where the resources are running.

4) Security concern 4: It is difficult to maintain the consistency of security and ensure the audit ability of records with the dynamic and fluid nature of virtual machines.

5) Security concern 5: There should be a common standard to ensure the integrity of data.

6) Security concern 6: Company violates the law (i.e. risk of data seizure by the (foreign) government).

7) Security concern 7: For the users to be sure that they are protected they must be regularly updated with application improvement.

8) Security concern 8: There are certain strict limits by some government regulations on what kind of data about its citizens can be stored and for how long, and the customer's financial data should remain in their home country is the condition required by some banking regulators.

9) Security concern 9: Logically the encryption and decryption keys should be controlled by the customers.

Various security issues are associated with cloud computing and they can be grouped into any number of dimensions.

In 2008 Gartner [9] said, the users should ask the vendors for seven specific security issues before they make a choice of cloud vendors and those seven security issues are Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, and long-term viability.

The security and privacy practices of some of the major cloud providers (such as Salesforce.com, Amazon, Google, and Microsoft) were evaluated by Forrester Research Inc.

[10] in 2009 in three major aspects: Security and privacy, compliance, and legal and contractual issues. For information assurance in the cloud, Cloud Security Alliance (CSA) [11] is gathering non-profits, individuals, and solution providers for getting into the discussion about the current and future best practices for clouds.

The thirteen domains of concerns on cloud computing security have been identified by CSA [12]. In 2011, investigations were made by S. Subashini and V. Kavitha on cloud computing security challenges from the cloud computing service delivery models (SPI model), and a detailed analysis and assessment method description for each security issue was given [13].

The cloud computing security issues were explored from different perspectives by Mohamed Al Morsy, John Grundy, and Ingo Müller in 2010, which included security issues associated with cloud computing architecture, service delivery models, cloud characteristics and cloud stakeholders [14].

Yanpei Chen, Vern Paxson, and Randy H. Katz believed that the complexities of multi-party trust considerations and the ensuing need for mutual audit ability are the two aspects that are to some degree new and essential to cloud. Some new opportunities in cloud computing security are also pointed out by them [15].

A large number of standard bodies with different interests currently exists and for promoting the wide use of cloud computing those bodies need to have a discussion and they should also work together for establishing common standards. In the below-specified domains, the possible "Inter-cloud" standards are needed to increase cloud interoperability and free data movement between clouds

- Network Architecture,
- Data Format,
- Metering And Billing,
- Quality Of Service,
- Resource Provisioning,
- Security, Identity Management And Privacy

Various general computing standards may be reused in the cloud but there are no dedicated cloud standards to our knowledge. This is something that must be addressed in the future and may add to the confusion for cloud users [16].

User data integrity and confidentiality should be attained while the data is stored in the cloud systems and these two are the major concerns that should be guaranteed.

IV General Vulnerabilities, Threats, and Attacks in Cloud

Cloud computing, like other areas of IT, suffers from several security issues, which need to be addressed. These risks pertain to policy and organization risks, technical risks, and legal and other risks.

Vulnerabilities and open issues

a) Cloud is a set of technology, process, people, and commercial construct. Like all other technology, process, people, and commercial construct, the cloud has vulnerabilities. The following are some of the vulnerabilities in a cloud. Some of the open issues and threats that need urgent attention are as follows:

b) Shared Technology vulnerabilities – increased leverage of resources gives the attackers a single point of attack, which can cause damage disproportional to its importance. An example of share technology is a hypervisor or cloud orchestration.

c) Data Breach – with data protection moving from cloud consumer to cloud service provider, the risk of accidental, malicious, and intentional data breach is high.

d) Account of Service traffic hijacking – one of the biggest advantages of the cloud is accessed through the Internet, but the same is a risk of

account compromise. Losing access to the privileged account might mean a loss of service.

e) Denial of Service (DoS) – any denial of service attack on the cloud provider can affect all tenets

f) Malicious Insider – a determined insider can find more ways to attack and cover the track in a cloud scenario.

g) Internet Protocol – many vulnerabilities inherent in IP such as IP spoofing, ARP spoofing, DNS Poisoning are real threats.

h) Injection Vulnerabilities – vulnerabilities such as SQL injection flaw, OS injection, and LDAP injection at the management layer can cause major issues across multiple cloud consumers.

i) API & Browser Vulnerabilities – Any vulnerability in the cloud provider's API or Interface poses a significant risk when coupled with social engineering or browser-based attacks; the damage can be significant.

j) Changes to Business Model – cloud computing can be a significant change to a cloud consumer's business model. IT departments and businesses need to adapt or face exposure to risk.

k) Abusive use – certain features of cloud computing can be used for malicious attack purposes such as the use of a trial period of use to launch zombie or DDoS attacks.

l) Malicious Insider – a malicious insider is always a major risk, however, a malicious insider at the cloud provider can cause significant damage to multiple consumers.

m) Availability –the probability that a system will work as required and when required.

Attack Vectors

According to a recent research8, the three major vectors of attack are network, hypervisor, and hardware. These vectors are mapped to attacks such as external, internal, and cloud providers or insider attacks respectively.

IV Countermeasures & Controls

The vulnerabilities and threats in the cloud are well documented. Each cloud service provider and cloud consumer has to devise countermeasures and controls to mitigate the risks based on their assessment. However, the following are some of the best practices in countermeasures and controls that can be considered:

a) End-to-end encryption – the data in a cloud delivery model might traverse through many geographical locations; it is imperative to encrypt the data end-to-end.

b) Scanning for malicious activities – end-to-end encryption while highly recommended, induces new risks, as encrypted data cannot be read by the Firewall or IDS. Therefore, it is important to have appropriate controls and countermeasures to mitigate risks from malicious software passing through encryption.

c) Validation of cloud consumer – the cloud provider has to take adequate precautions to screen the cloud consumer to prevent important features of cloud being used for malicious attack purposes.

d) Secure Interfaces and APIs –interfaces and APIs are important to implement automation, orchestration, and management. The cloud provider has to ensure that any vulnerability is mitigated.

e) Insider attacks – cloud providers should take precautions to screen employees and contractors, along with strengthening internal security systems to prevent any insider attacks.

f) Secure leveraged resources – in a shared/multi-tenancy model, the cloud provider has secure shared resources such as a hypervisor, orchestration, and monitoring tools.

g) Business Continuity plans – Business continuity plan is a process of documenting the response of the organization to any incidents that cause the unavailability of whole or part of a business-critical process.

V Conclusions

Security in cloud computing is evolving in step with risks as they are discovered often too late to prevent incidents. Cloud computing due to its disruptive nature, complex architecture, and leveraged-resources pose a unique and severe risk to all actors. All stakeholders and actors must understand the risk and mitigate it appropriately. Security needs to be built at every layer in a cloud-computing platform by incorporating best

practices and emerging technologies to effectively mitigate the risk. In the cloud, consumer, provider, broker, carrier, auditor, and everyone else has to take the necessary precautions against risks to truly secure the cloud-computing platform or be exposed to significant and sometimes business-critical risk. According to a recent survey, the industry recognizes that security engineering provides best practices, methods, and techniques for developing systems and services, which are built for security, sustainability, and resiliency. It is important to take this research forward to provide such best practices to more applications and use cases. It is also essential to conduct further research in systems development life cycle (SDLC) for cloud consumers to incorporate various development and technological advancement models and container systems such as Docker to improve security at a fundamental level. Additionally, there is very limited research on training and people's impact on security. Work can be done to understand the challenges, requirements, and impact of effective security training for consumers and other providers

References

[1] National Institute of Standards and Technology. The NIST definition of cloud computing; 2011.

[2] Mell Peter, Grance Tim. Effectively and securely using the cloud computing paradigm; 2011.<http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt> [retrieved 18.04.20].

[3] Baek Sung-Jin, Park Sun-Mi, Yang Su-Hyun, Song Eun-Ha, Jeong Young-Sik. Efficient server virtualization using grid service infrastructure. J Inform Process Syst 2010;6(4):553–62.

[4] Klyuev Vitaly, Oleshchuk Vladimir. Semantic retrieval: an approach to representing, searching, and summarising text documents. Int J Inform Technol Commun Converg 2011;1(2):221–34.

[5] Nyre Åsmund Ahlmann, Jaatun Martin Gilje. A probabilistic approach to information control. J Internet Technol 2010;11(3):407–16.

[6] Ling Amy Poh Ai, Masao Mukaidono. Selection of model in developing information security criteria for smart grid security system. J Converg 2011;2(1):39–46.

[7] M. Casassa-Mont, S. Pearson, and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services", Proc. DEXA 2003, IEEE Computer Society, 2003, pp. 377-382.

[8]https://www.pcisecuritystandards.org/index.shtml.

[9] Gartner: Seven cloud-computing security risks. InfoWorld., http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853.

[10] Cloud Security Front and Center. Forrester Research. 2009-11-18.http://blogs.forrester.com/srm/2009/11/cloud-security-front-andcenter.html.

[11] Cloud Security Alliance. http://www.cloudsecurityalliance.org.

[12] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, 2012.

[13] S. Subashini, V.Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34(2011)1-11.

[14] Mohamed Al Morsy, John Grundy, Ingo Müller, "An Analysis of The Cloud Computing Security Problem," in Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[15] Yanpei Chen, Vern Paxson, Randy H. Katz, "What's New About Cloud Computing Security?" Technical Report No. UCB/EECS-2010-5. http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/ EECS-2010-5.html.

[16] Fogarty Kevin. Cloud computing standards: too many, doing too little; 2011. <http://www.cio.com/article/679067/,Cloud_Computing_Standards_Too_Many_Doing_Too_Little> [retrieved 15.06.20].