International Journal of Engineering & Technology, 7 (2.4) (2018) 88-92

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A Survey on Security and Privacy Issues in Cloud Computing

T. Thilagam[1*] , K. Arthi[2] , C. Amuthadevi[3]

Research Scholar[1] and Associate Professor [2,3], Department of Computer Science
Veltech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Chennai, Tamil Nadu, India.
**Email: thilaka28@gmail.com*

Abstract

Cloud computing is broadly utilized rising innovation for putting away and sharing information over web yet at the same time confronting loads of security and protection issues. These difficulties incorporate client's mystery information misfortune, information spillage and uncovering of the individual information security. Considering the security and protection inside the cloud there are different dangers to the client's delicate information on distributed storage. This paper is review on the security and protection issues and accessible arrangements. Additionally present diverse open doors in security and protection in cloud condition. Furthermore, cloud specialist co-ops (CSPs) can likewise deliver the talked about issues to offer better security and protection.

Keywords: *Cloud Computing, Security, Privacy, Cloud Service Providers*

1.Introduction

Cloud is widely used for storing, backing up and sharing information. There are many benefits to use cloud storage. Information put away in the cloud can be gotten to whenever from wherever as long at any as there is organize get to. For example, buying extra storage limit, can be offloaded to the obligation of a specialist co-op. Regardless of its points of interest, outsourcing information storage likewise expands the assault surface region in the meantime. For instance, when information is disseminated, the more areas it is put away the higher hazard it contains for unapproved physical access to the information. By offering storage and systems to numerous different clients it is additionally workable for other unauthorized clients to get to your information. Encryption can ensure information as it is being transmitted to and from the cloud benefit. It can additionally secure information that is put away at the specialist co-op. Indeed, even there is an unauthorized users who has accessed the cloud, as the information has been encoded, the foe can't get any data about the original text. Asymmetric encryption permits the scramble or to utilize just people in general data to produce a figure content while the beneficiary uses his/her own mystery key to decrypt. Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and, more broadly, information security.

1.1 Types of cloud services

Most cloud computing services fall into three broad categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (Saas). These are sometimes called the cloud computing stack, because they build on top of one another. Knowing what they are and how they are different makes it easier to accomplish your business goals[17].

Infrastructure-as-a-service (IaaS)
The most basic category of cloud computing services. With IaaS, you rent IT infrastructure—servers and virtual machines (VMs), storage, networks, operating systems—from a cloud provider on a pay-as-you-go basis[17].

Platform as a service (PaaS)
Platform-as-a-service (PaaS) refers to cloud computing services that supply an on-demand environment for developing, testing, delivering and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network and databases needed for development[17].

Software as a service (SaaS)
Software-as-a-service (SaaS) is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching.

Users connect to the application over the Internet, usually with a web browser on their phone, tablet or PC[17].

1.2 Cloud Deployments Models:

[17] Not all clouds are the same. There are three different ways to deploy cloud computing resources: public cloud, private cloud and hybrid cloud.

Public cloud
Public clouds are owned and operated by a third-party cloud service provider, which deliver their computing resources like servers and storage over the Internet. Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software and other supporting infrastructure is owned and managed by the cloud provider. You access these services and manage your account using a web browser.

Private cloud
A private cloud refers to cloud computing resources used exclusively by a single business or organization. A private cloud can be physically located on the company's on-site datacenter. Some companies also pay third-party service providers to host their private cloud. A private cloud is one in which the services and infrastructure are maintained on a private network.

Hybrid cloud
Hybrid clouds combine public and private clouds, bound together by technology that allows data and applications to be shared between them. By allowing data and applications to move between private and public clouds, hybrid cloud gives businesses greater flexibility and more deployment options.

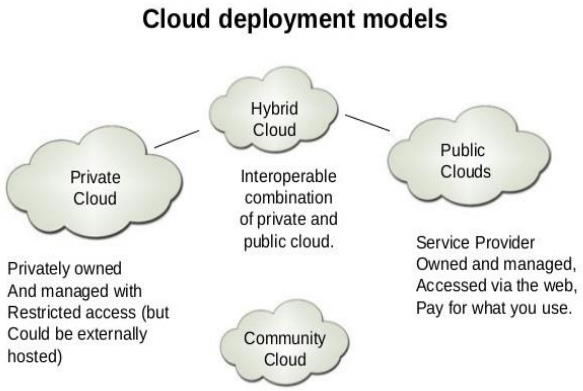

Figure 1: Cloud Deployment model

2. Related work

In [7] "Security and Privacy issues in cloud computing" the authors reviewed cloud computing technology, its deployment and service models. They also focused on key security and privacy issues that affect cloud computing.

In [8] "Challenges and Security issues in cloud computing from two perspectives: Data security and Privacy protection" the authors focused the difficulties and security issues in cloud computing from the information security and privacy protection viewpoint.

In "Security and Privacy in Cloud Computing: Vision, Trends, and Challenges" by [3]theauthors focused on some of a portion of the difficulties and constraints of cloud security, concentrating on information use administration perspectives and access control.

[1]In this paper titled Security and Privacy in Cloud Computing, discussed related challenges, opportunities, and solutionsrelating to cloud security and privacy.

[9]in this paper "On Current Trends in Security and Privacy of Cloud Computing" analyzed privacy and security requirements in cloud computing and suggested open research areas in cloud computing systems. [10]in their paper titled "Evaluating Security and Privacy in Cloud Computing Services: A Stakeholder's Perspective", identified and categorized cloud security and privacy attributes. These categorized features were then used to define the expectations from cloud computing service providers so that consumers could make well educated choices.

[2] in their paper titled Security and Privacy Challenges in Cloud Computing Environments, explored the roadblocks and solutions to providing a trustworthy cloud computing environment. [4]in their paper titled "Security and Privacy in Cloud Computing: A Survey" discussed with several Cloud Computing service providers about their security and privacy concerns. They observed that the security and privacy concerns presented by most cloud computing system providers were not adequate. They proposed the deployment of more security strategies in the cloud environment to achieve the desired control, availability, confidentiality and data integrity. They also proposed a modification in that privacy acts to enhance the relationship between cloud providers and users.

3. Security and Privacy

3.1 Identity administration

Each undertaking will have its own particular character administration framework to control access to data and figuring assets. Cloud suppliers either incorporate the client's character administration framework into their own particular foundation, utilizing league or SSO innovation, or a biometric-based distinguishing proof system, [1] or give a personality administration arrangement of their own. Cloud ID, for example, gives protection saving cloud-based and cross-endeavor biometric distinguishing proof. It interfaces the secret data of the clients to their biometrics and stores it in a scrambled manner. Making utilization of an accessible encryption procedure, biometric distinguishing proof is performed in encoded area to ensure that the cloud supplier or potential assailants don't access any delicate information or even the substance of the individual questions.

3.2 Physical security

Cloud specialist organizations physically secure the IT equipment (servers, switches, links and so forth.) against unapproved get to, obstruction, burglary, fires, surges and so on and guarantee that fundamental supplies, (for example, power) are adequately strong to limit the likelihood of interruption. This is typically accomplished by serving cloud applications from 'world-class' (i.e. professionally determined, planned, developed, oversaw, checked and kept up) server farms.

3.3 Personnel security

Different data security concerns identifying with the IT and different experts related with cloud administrations are commonly taken care of through pre-, Para-and post-business exercises, for example, security screening potential enlisted people, security mindfulness and preparing programs, proactive.

3.4 Privacy

Suppliers guarantee that every basic datum (Mastercard numbers, for instance) are conceal or scrambled and that lone approved clients approach information completely. In addition, advanced characters and certifications must be secured as should any information that the supplier gathers or delivers about client movement in the cloud.[14]

4. Benefits of Cloud Computing

Cloud computing is a major shift from the traditional way businesses thinking about IT resources. Main benefits of cloud computing and also some common reasons organizations are turning to cloud computing services:

• Cost
Cloud computing disposes of the capital cost of purchasing equipment and programming and setting up and running nearby data centers—the racks of servers, the round-the-clock power for power and cooling, the IT specialists for dealing with the framework. It includes fast.
• Speed
Most cloud computing administrations are given self-administration and on request, so even immense measures of processing assets can be provisioned in minutes, commonly with only a couple of mouse clicks, giving organizations a great deal of adaptability and taking the weight off capacity planning.
• Global scale
The main advantages of cloud computing administrations incorporate the capacity to scale flexibly. In cloud talk, that implies conveying its perfect measure assets—for instance, pretty much registering power, storage, data transfer bandwidth—right when its required and from the privilege geographic area.
• Productivity
On location datacenters ordinarily require a ton of "racking and stacking"— equipment set up, programming fixing and other tedious IT administration errands. Distributed computing expels the requirement for a considerable lot of these errands, so IT groups can invest energy in accomplishing more critical business objectives.
• Performance
The greatest cloud computing administrations keep running on an overall system of secure datacenters, which are consistently moved up to the most recent age of quick and productive registering equipment. This offers a few advantages over a solitary corporate datacenter, including lessened system inactivity for applications and more prominent economies of scale.
• Reliability
Cloud computing makes information reinforcement, fiasco recuperation and business progression simpler and more affordable, on the grounds that information can be reflected at various excess destinations on the cloud supplier's system.
• Self-benefit provisioning
End clients can turn up register assets for a workload on request. This kills the customary requirement for IT overseers to arrangement and oversee register assets.
• Elasticity
Organizations can scale up as figuring needs increment and scale down again as requests diminish. This takes out the requirement for gigantic interests in nearby foundation, which might possibly stay dynamic.
•Pay per utilize
Register assets are estimated at a granular level, empowering clients to pay just for the assets and workloads they utilize.
•Workload flexibility
Cloud specialist organizations regularly execute excess assets to guarantee versatile capacity and to keep clients' vital workloads running - frequently over numerous worldwide districts.
• Relocation adaptability
Organizations can move certain workloads to or from the cloud - or to various cloud stages - as wanted or consequently for better cost investment funds or to utilize new administrations as they develop.

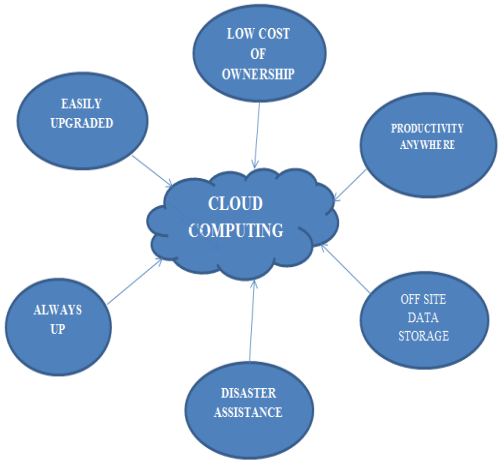

Figure 2: Benefits of Cloud Computing

Figure 2 shows some of the benefits of cloud computing. The cloud can cater for as many services as are required. There are no limits to the number of services that can be deployed and so cloud users can enjoy the functionalities of many services. Another huge advantage is that services are stored in a distributed fashion. i.e. The storage of cloud data is not restricted to any particular location [6] Examples of some well-known cloud computing providers are Amazon, Microsoft Azure and Google.

5. Cloud Privacy and Security Issues

5.1. Network and Data Security

Network and data security in cloud computing has several facets such as data confidentiality, integrity, availability and backup and disaster recovery. These are briefly discussed below:
Data Confidentiality: Data confidentiality is a key issue to be considered when outsourcing highly sensitive data to the cloud. Confidential data should be inaccessible to unauthorized users and one way of ensuring confidentiality is by the use of strict access control policies. Policies should be in place to prevent

unauthorized users from inferring anything from the information being stored in the cloud database. Data confidentiality is achieved through encryption of data. With data encryption however, there is the issue of key distribution / management of keys. Different encryption algorithms have been proposed such as Rivest Shamir Adelman (RSA), Triple Data Encryption Standard (3DES) and Homomorphic encryption. In Homomorphic encryption, computations are carried out on encrypted data (cipher text), [16] thus generating an encrypted result, which, when decrypted, matches the result of the same operations performed on the original data (plaintext). This can be a most important advantage for applications that outsource encrypted data to the cloud. The major drawback of this method is its computational complexity and cost [3].

Data Integrity: The term integrity explains the wholeness and completeness of data which is a key issue in IT systems. It is the process of verifying data. It guarantees the quality and correctness of data. In cloud computing the integrity of data storage is a necessary and important requirement. The integrity of data proves its regularity, consistency and validity. As the cloud service requirements increase, the CSP may need to scale up their storage systems and this may lead to high chance of data loss, data corruption, disk failure, node failure or hardware failure. Thus, monitoring data integrity in cloud is so important to prevent the possibilities of data crash and corruption. It is easier to achieve data integrity in centralized systems than in distributed cloud computing environment. Data integrity can be ensured by auditing processes. A cloud auditor independently evaluates cloud services and cloud infrastructure. Periodic third party auditing mechanisms could be initiated to verify data integrity data integrity [7].

Data Availability: The service created for users must be available to them when needed. However, some situations exist in which data availability cannot be guaranteed. For example, in unavoidable situations like natural disasters, it is important to know if the data can be utilized, verified or recovered by the data owners. The cloud customers must be aware of the security measures being taken by the cloud service provider. They should also read the fine print of the Service Level Agreement (SLA) entered into with the service providers. [6] High availability in cloud infrastructures can be achieved by designing fault-tolerant cloud systems. Cloud systems should be designed for server failure, zone failure and cloud failure.

Backup & Disaster Recovery: It is essential for CSP's to provide a backup and disaster recovery plan for data protection, recovery, resiliency of data centre, data availability and to allow business continuity after network or system failures. The cloud users must be informed about the backup type and requirements and what disaster recovery plan is available.

5.2. Governance, Compliance and Legal Issues.

The physical location of the server farm and cloud infrastructures should be confidential as physical security of infrastructure is also very important. The CSP must have a procedure or set of procedures to secure customers' data if there is a suspected threat or breach and this must be shared with the customers upon request. In addition, the sanitization of data stored in the cloud is a critical issue to be discussed. Cloud users should be assured their data will always be secure even if the cloud service providers collapse or are acquired by another company. Cloud users should also know how they can obtain their data back and in what format [13]. Compliance refers to an organizations' responsibility to operate. Compliance is a tricky and somewhat complicated subject in cloud computing because security and privacy laws and regulations vary from region to region [9]. What might be legal in certain regions might be considered illegal in other areas. Cloud customers should understand the terms and references of any service level agreement (SLA) entered into with the CSP or CSP's in the case of nested services (when a consumer gets different services from different vendors) in its entirety, including penalties for defaulting and mode of compensation.

5.3. Communication Interface & Virtualization Security

The cloud user has a part to play in ensuring security of cloud services. This is so because the nature of connections and devices used by the cloud user to connect to the cloud has its own security implications. For example, wired / wireless connections, using secure browsers etc. In addition, authentication of users only provides a proof of identity. It does not limit the actions or operations that a legitimate user of a computer system can perform. So an authenticated user may carry out some unauthorized operations if auditing and access control measures and policies are not introduced. Furthermore, in multi-tenancy, hypervisors ensure that multiple operating systems, can run concurrently on a single physical machine. The different operating systems may be owned by different customers called tenants. This method of sharing physical resources could also introduce some vulnerability and the cloud users should know if the CSP's can identify and defend side-channel attacks? [10]

6. Conclusion and Future Works

Cloud computing includes getting to a mutual pool of arranged processing framework and assets. The cloud offers advantages, for example, lessened costs, decreased administration duties, increments hierarchical productivity and so forth. Regardless of the numerous points of interest related with distributed computing, there are much helplessness for cloud protection and security. In this paper cloud administration and arrangement models was talked about. This paper likewise recognized the key security and protection issues in distributed computing and examined arrangements. Because of the complexities of the cloud, it might be hard to accomplish end-to-end protection and security and this may turn out to be an obstacle for appropriation of distributed computing frameworks. A testing research region open for scientists is insider put stock in issues in CSP's. Trust issues include a cloud supplier manager utilizing the chairman record to attack the shopper's cloud security as well as protection. Promote endeavors can be directed towards guaranteeing adherence administrative consistence structures and better non-divulgence standards by the cloud suppliers to ensure broad business accomplishment of cloud administrations.

References

[1] Z. Tari, "Security and Privacy in Cloud Computing,"IEEE Cloud Comput., vol. 1, no. 1, pp. 54–57, 2014.

[2] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Secur. Priv. Mag., vol. 8, no. 6, pp. 24–31, 2010.

[3] Z. Tari, X. Yi, U. S. Premarathne, P. Bertok, and I. Khalil, "Security and privacy in cloud computing: Vision, trends, and challenges," IEEE Cloud Comput., vol. 2, no. 2, pp. 30–38, 2015.

[4] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and Privacy in Cloud Computing?: A Survey Security and

Privacy in Cloud Computing:," Sixth Int. Conf. Semant. Knowl. Grids, vol. 2, pp. 126–149, 2010.

[5] W. Kong, Y. Lei, and J. Ma, "Data Security and Privacy in Cloud Computing," Int. J. Distrib. Sens. Networks, vol. 2014, pp. 512–514, 2014.
[6] Arjun and Vinay, "A Short Review on Data Security and Privacy Issues in Cloud Computing," IEEE, 2016.
[7] M. M. U. B. YahyaKord, TamandaniQahtan, "Security and Privacy Issues in Cloud Computing," IEEE, pp. 896–900, 2016.
[8] S. Mahdi Shariati, M. Abouzarjomehri, and H. Ahmadzadegan, "Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection," 2nd Int. Conf. Knowledge-based Eng. Innov., pp. 1078–1082, 2015.
[9] S. Sahin, "On Current Trends in Security and Privacy of Cloud Computing," Proc. AICT'13, pp. 1–5, 2013.
[10] Abuhussein, H. Bedi, and S. Shiva, "Evaluating Security and Privacy in Cloud Computing Services: A Stakeholder's Perspective," Internet Technol. Secur.Trans., pp. 388–395, 2012.
[11] G. Kulkarni, N. Chavan, R. Chandorkar, R. Waghmare, and R. Palwe, "Cloud security challenges," Telecommun. Syst. Serv. Appl. (TSSA), 2012 7th Int. Conf., pp. 88–91, 2012.
[12] J. Kozhipurath,"Cloud Service Costing Challenges," IEEE, 2012.
[13] P. K. G. Gandhi, "Cloud Computing Security issues: An Analysis," IEEE, pp. 3858–3861, 2016.
[14] Mahesh U. Shankarwar and Ambika V. Pawar, "Security and Privacy in Cloud Computing: A Survey", © Springer International Publishing Switzerland 2015.
[15] Joseph K. Liu, Kaitai Liang∗ , Willy Susilo, Jianghua Liu, Yang Xiang,"Two-Factor Data Security Protection Mechanism for Cloud Storage System", ieee-tc-2016.
[16] ZahirTari, Xun Yi, Uthpala S. Premarathne, Peter Bertok, Ibrahim Khalil. "Security and Privacy in Cloud Computing: Vision, Trends, and Challenges", IEEE Cloud Computing, 2015
[17] https://www.wikipedia.org