IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007202|

Cloud Computing and Security Issues — A Review of Amazon Web Services

Punit Kumari

Assistant Professor (HOD-IT Department), Innocent Hearts Group of Institutions, Loharan, Punjab, India

ABSTRACT: Cloud computing is a collection of different services that we can avail when we require. These services can be a tools and applications such as databases, servers, data storage, networking and software's. Almost every people in this world use cloud but they are known like using emails, use of mobiles apps and many more. All types of Organizations and industries are using this facility instead buying physical things like servers, computers, storage devices, hard drives, own infrastructure of networks. Basically, a cloud computing is a collection of networks or it is just an allegory of internet. In this paper I am going to describe about security issues of cloud computing and the services provided by Amazon cloud server. This research paper also analyzes the challenges the AWS is facing and trying to solve these issues.

KEYWORDS: cloud computing, cloud servers, challenges (Abstract web service),

I. INTRODUCTION

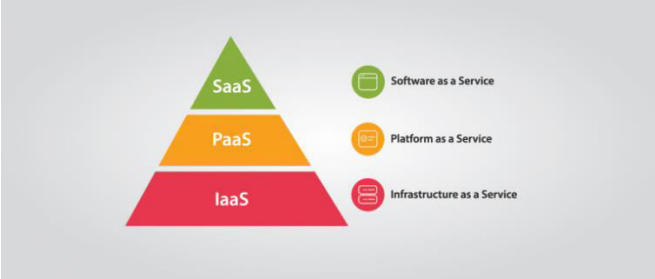
Cloud computing is the latest trend of services and resources providing through cloud computing. All this is done through Cloud service providers (CSP). CSP 's provides platform to customers for all resources and services on demand similar to internet service provider (ISP) offer costumers high speed broadband to access the internet. In cloud-based infrastructure, the resources and services are on someone else network or premises and platform and assessed remotely by cloud users. In some situations, someone have requirement to store data on remote server. These scenarios breaches three types of states: -

- Personal sensitive data transmission to the cloud server.
- The dispatch of data from the cloud server to clients' computers
- Personal sensitive data storage on cloud server without owned it.

All these states show the security is the main concern in cloud computing. The aspects presented in this paper are organized with a view to discuss and identify the approach of different cloud platform to cloud computing.Security issues derived in cloud computing approach have been discussed afterwards. After thatdiscussion of services provided by Amazon cloud server and its challenges and solutions has also beenincluded.

Cloud Service Model

- SaaS (Software as a Service)
- IaaS (Infrastructure as a Service)
- PaaS (Platform as a Service).



Every cloud model has their own set of facilities that could serve the needs of various businesses.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007202|

1. **SaaS (Software as a service)-**This model provides fast access of cloud-basedweb applications to the clients. These applications can run on the cloud and you can only use them by a paid licensed subscription or for free with limited access. For instance, SaaS includesGmail account, Google G Suite, Microsoft Office 365, Dropbox etc.
2. **IaaS (Infrastructure as a Service)**- IaaS or Infrastructure also known as hardware as a service. This Service is basically a virtual provision of computing resources over the cloud. An IaaS cloud provider can provide you infrastructures such as storage, servers, networking hardware alongside maintenance and support. Amazon Web Services, Microsoft Azure, and Google Compute Engine are some of the leading IaaS cloud service providers.
3. **PaaS (Platform as a Service)-** Platform as a Service or PaaS is essentially a cloud base where you can develop, test and organize the different applications for your business. The virtual runtime environment provided by PaaS gives a favourable space for developing and testing applications. These resources offered in the form of servers, storage and networking are manageable either by the company or a platform provider. Google App Engine and AWS Elastic Beanstalk are two typical examples of PaaS.

II. LITERATURE REVIEW

Armbrust, et al. (2009) and Cachin, Keidar and Shraer (2009) allude to the 2008 flop of The Linkup, an online storage administration, as a most exceedingly terrible case sample of a cloud computing storage supplier going out of business. To mellow the blow of such disturbances, the Cloud Security Alliance (2009) prescribes that cloud computing clients might as well think about having an exchange area that can undertake the services long ago rendered by the cloud computing administration supplier (p. 50). Such an area could either be the client's own data focus, or at an alternate cloud computing administration supplier site.

Viega (2009) likewise states that clients may as well keep up their own reinforcements notwithstanding those taken by the cloud computing administration supplier, however includes that it is ordinarily less demanding with IaaS than with PaaS or SaaS.

Abadi (2009) states that clouds are ordinarily based top of shoddy, thing hardware, for which washout is not phenomenal. Thus, the likelihood of a washout happening throughout a long running data dissection errand is moderately high (p. 6).

Finnie (2008) states that cloud computing is a minefield for most chief information officers and information technology associations (p. 22), implying that the effect from the misfortune of control may accelerate the powerlessness to consent to security prerequisites, an absence of secrecy, trustworthiness, and accessibility of data, a crumbling of execution and nature of administration, and the presentation of consistence tests (ENISA, 2009, p. 28). A hefty portion of the heading cloud administration suppliers don't acknowledge authority regarding the data archived in their infrastructure, which implies that they additionally don't acknowledge any transference of danger (Cloud Security Alliance, 2009, p. 26).

Data Sources

There are two types of data sources available to the research processes.

1. Primary data 2. Secondary data

III. OBJECTIVE OF STUDY

Secondary objectives

1. Security issues of Cloud computingservices.
2. Different Amazon Web Services and its uses, its Challenges and solutions

Security issues with cloud computing services

A study in [3] have discussed security risks, vulnerabilities, and attacks, with reference to overall networks in general and cloud computers. Among many security attacks, the authors found that the there are several types of attack on cloud computers affecting their confidentiality, integrity, and availability. The most common type of attack is the denial of service (DOS) [4]. A DOS attack makes a given cloud owner's resources unavailable to them and their users. The authors explain that a security flaw in a cloud infrastructure can have more devastating effects, because hardware and other resources are shared on a cloud. A breached system can spread its effects to other systems that might belong to

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007202|

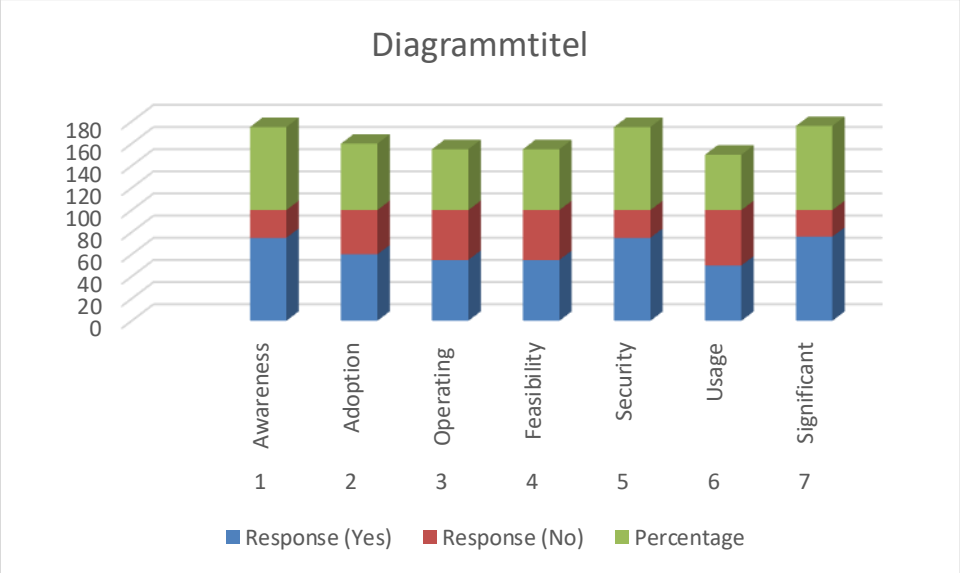
someone else using the same cloud storage. Hence, it potentially impacts a large population [5]. Some of the security attacks, like finding encryption keys, getting to know about plain text, and other cryptographic attacks affect only the machine owner's data. They have lesser or no effect on other cloud server users [6]. One of the biggest security risks involved with cloud computing is the element of trust. This is because the service user is not buying, configuring, monitoring, and implementing their own personal computers and servers physically. These services are provided to them on request by a cloud computing service provider. This makes their configuration and internal settings vulnerable to the services on which they rely. This situation can lead to an attack on the confidentiality and/or integrity of the data present in the cloud [7]. In [8], the authors have elaborated on the significant risks involved with cloud services in particular.

Services provided by Amazon Web server

Amazon Web Services offers a broad set of global cloud-based products including compute, storage, databases, analytics, networking, mobile, developer tools, management tools, IoT, security, and enterprise applications: on-demand, available in seconds, with pay-as-you-go pricing. From data warehousing to deployment tools, directories to content delivery, over 140 AWS services are available. New services can be provisioned quickly, without the upfront capital expense. This allows enterprises, start-ups, small and medium sized businesses, and customers in the public sector to access the building blocks they need to respond quickly to changing business requirements.

TABLE 1. ANALYSIS OF FACTORS INFLUENCING USAGE OF AWS SERVICES

S.no	Services	Response (Yes)	Response (No)	Percentage
1	Awareness	75	25	75
2	Adoption	60	40	60
3	Operating	55	45	55
4	Feasibility	55	45	55
5	Security	75	25	75
6	Usage	50	50	50
7	Significant	76	24	76



Inference: -The primary data collected specifies that awareness of AWS services is 75 %. whereas who adopted are 60%.55% users are operating the services simultaneously, agrees usage is feasible and secured.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007202|

Challenges and solutions of AWS

- **Identify the key objectives of business before migrating to cloud**
  The major concern and challenge of each businesses to determine the main features and functionalities that need during migration to cloud. The applications and tools of AWS should be compatible with your business.
- **Adoption of new technology**
  The smooth incorporation of application with AWS depends on the acceptance of the users. Firstly, each business should understand the benefits of the changes in technologies and also convinced their team to adopt it for get advantages from cloud.
- **Security and data protection**
  Today's scenario data security is a major concern. Data is a biggest asset of any company or enterprise. While migration slight carelessness could lose your data while migration time. To prevent this happen you should decide what type of data you should store in the cloud and where it is residing after migrated. All these questions should be cleared from the AWS certified developer before the migration.
- **Recognized overall cost early**
  Many organizations fail to estimate the which services /job should be transfer to cloud that why the false cost prediction measured, AWS cost varies depending on the type and of services and number of users. Hence companies have to decide earlier before sending data on the cloud. You can send firstly less used applications because moving of data is a slower process and you can save money.
- **Getting right quality and performance**
  Right quality, performance and reliability is most important for migration process. Choosing the right AWS consulting partner is very crucial. All required features, less downtime and quick access need to be kept in mind before migration.

IV. CONCLUSION

From this research paper I conclude that cloud computing has may issues regarding security, cost effectiveness scalability and many more but by using AWS we can vanish all these problems.Another possible solution to the above-mentioned security issues can be that AWS should not allow services and clients to share account login information with each other.AWS gives its clients full control of an instance, it can be concluded that security is not only the responsibility of the cloud provider, but also of the client. Human beings are the weakest link, as they say. AWS gives you flexibility which means you need not to worry about compute, processing, data storage, data security and integrity. It automatically scale up their cloud servers if data size increses.it also gives free tier access of aws console initially for a one year to get handy of using aws services.

REFERENCES

1. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 4, April 2018, ISSN: 2278 – 1323
2. International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014
3. Varsha et al, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June- 2015, pg. 230-234
4. Hashizume et al. Journal of Internet Services and Applications 2013, 4:5 http://www.jisajournal.com/content/4/1/5
5. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 22 (2018) pp. 16077-16084 © Research India Publications. http://www.ripublication.com
6. "How Cloud Computing Works", [Online]. Available: http://computer.howstuffworks.com/cloudcomputing/cloud-computing.htm
7. Te-Shun C., 2013, "Security Threats on Cloud Computing Vulnerabilities", International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3.
8. Mosca, P., Zhang, Y., Xiao, Z. and Wang, Y. (2014) Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services. International Journal of Communications, Network and System Sciences, 7, 529-535.
9. Mutch, J., "How to Steal Data from the Cloud", 2010, [Online]. Available: http://www.cloudbook.net/resources/stories/how-tosteal-data-from-the-cloud
10. Archer J. (2010), "Top Threat to Cloud Computing", Cloud Security Alliance. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v 1.0.pdf

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007202|

11. Kirchgaessner S. (2013), Cloud Storage Carries Potent Security Risk, [Online]. Available: http://www.ft.com/cms/s/0/4729ed7c-3722-11e3-9603- 00144feab7de.html
12. Simonite T (2012) "How to steal data from your neighbor in the cloud". MIT Technology Review, 8 Nov 2012. www.technologyreview.com/news/506976/howto-steal-data-from-your-neighbor-in-the-Cloud/
13. Hanim. E. (2013), "Security threats and solutions in cloud computing," in 2013
14. World Congress on Internet Security, WorldCIS 2013, 2013, pp. 139–143.
15. International Journal of Trend in Scientific Research and Development (IJTSRD)
16. Volume: 3 | Issue: 3 | Mar-Apr 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470
17. International Journal of Trend in Scientific Research and Development (IJTSRD)
18. Volume: 3 | Issue: 3 | Mar-Apr 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 647[9] International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014
19. [10] Varsha et al, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June- 2015, pg. 230-234[11] International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 4, April 2018, ISSN: 2278 – 1323[12] International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 22 (2018) pp. 16077-16084 © Research India Publications. http://www.ripublication.com[13] ARPN Journal of Science and Technology ©2011-2013. All rights reserved.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details