Academic Guru Publication House

Advances in Cloud Computing Security
Techniques and Applications
Volume 1
Year: 2021

AG PH Books

Cloud Architectures Encountering Data Security and Privacy Concerns- A Survey

Ms. Shweta Singh[1*]

[1]*Cloud Computing, architecture, PaaS, SaaS, IaaS, Cloud Computing, Cloud Attacks, Cloud Security.*

Abstract

Emerging as one of the most relevant IT paradigms of recent times is cloud computing. The IT environment is increasingly being transformed by cloud computing. Cloud users may access resources, apps, including infrastructure from cloud providers on the pay-as-you-go basis. As an example, cloud providers may already have apps in place for their customers to utilise. As an example, the cloud service provider may provide the capacity to design and the deploy user apps. The Massive storage infrastructure is also accessible for such database and any user-provided data. There are a slew of different cloud designs, and more are on the way. SaaS, PaaS, as well as IaaS are by far the most common, and they may be set up in private, public, communal, or a mix of these environments. It explores current cloud computing architectural advances and gives a review of numerous investigations undertaken inside cloud computing industry to address various dangers inside its design, with specific reference towards multi-cloud architectures.

Keywords: Research, Methodology, Research Methodology, Research Techniques, Qualitative research, Quantitative Research.

1. INTRODUCTION

There is a growing trend toward the cloud computing, that minimises the administration burden on businesses and enables them to concentrate on their core functions. Cloud computing is one of top 10 computing advancements, according to the Gartner survey [1]. The computer resources, data, as well

* ISBN No. 978-81-955340-6-7

Copyrighted Material

as memory space provided by cloud computing are all extremely reasonably priced. Computing innovation provides numerous benefits over conventional privately held data centres, including commercial innovation, economies of scale, cheap administrative overhead, inexpensive operating as well as maintenance costs, with high quality services. In this regard, cloud computing seems to be an excellent alternative for many IT companies.

When it comes to storing data on cloud, cloud computing is employed by both small businesses as well as major corporations.

Service-oriented as well as event-driven architectures are combined in the cloud computing architecture.

The architecture of cloud computing is broken down into followings two sections: -

- Front End
- Back End

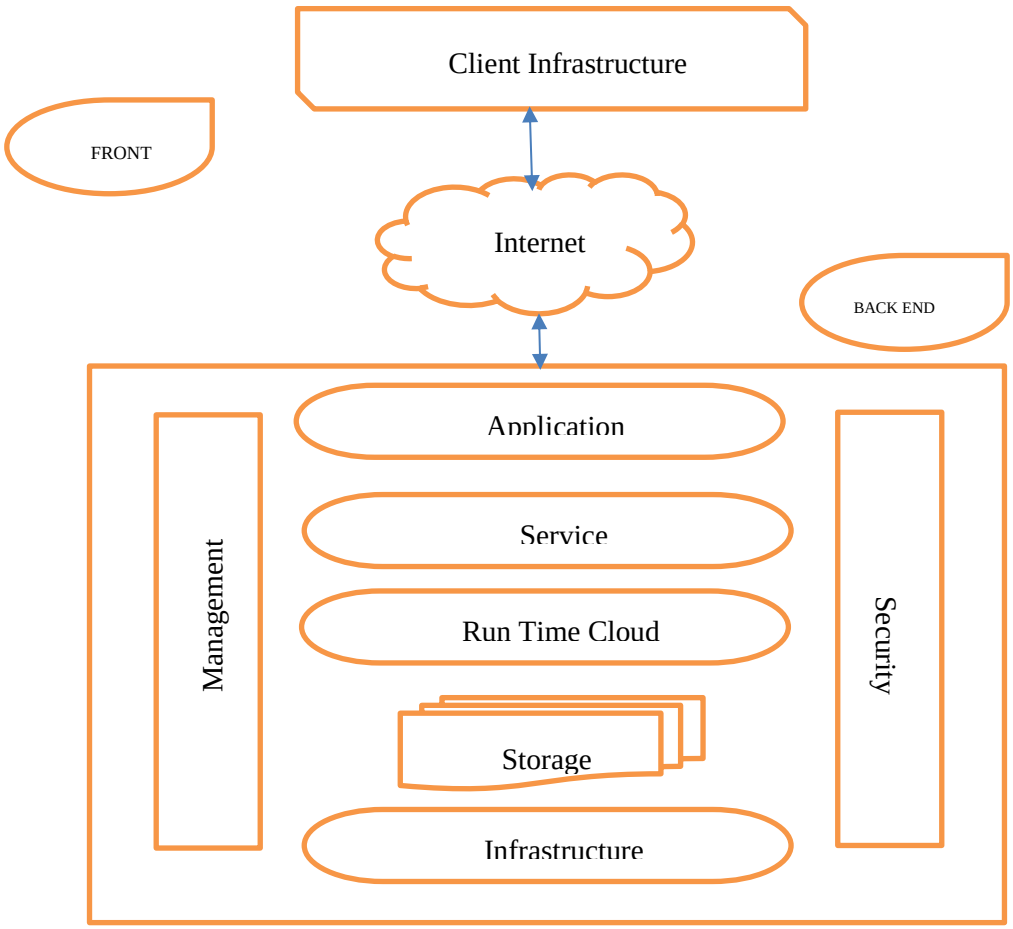

Figure 1: Cloud computing architecture

Copyrighted Material

Front End

The client interacts with front end. It has client-side APIs and applications needed to connect to the cloud computing infrastructures that are included inside. Web servers (such as Chrome, Firefox, and the Internet Explorer, among others) are part of front end, as are thin and the fat clients, the tablets, as well as mobile devices.

Back End

Service provider uses back end. To deliver cloud computing services, it oversees the management of all resources necessary for this to take place. Everything from data storage to the virtual computers to servers to the traffic control systems is included.

Small and medium-sized businesses may save money and time by using the cloud to run their businesses more effectively [2]. Cloud computing has had a slew of different definitions put out over the years. The online environment provides computer resources on-demand as well as that could be remotely controlled by a large number of people may be defined as a generic definition. Visual interfaces allow users to manage as well as control such assets, including storages, infrastructures (like servers and networks), licenced software, as well as services, as well as pay for them as they use them [3][4].

2. CLOUD SERVICES

IAAS stands for the Infrastructure as a Service, SAAS stands for the Software as a Service, while PAAS stands for Platform as a Service, overall of which are offered via the cloud. In general, the cloud provides three types of services to its users: Infrastructure as a Service represented as (IAAS), Software as a Service represented as (SAAS), and Platform as a Service represented as (PAAS).

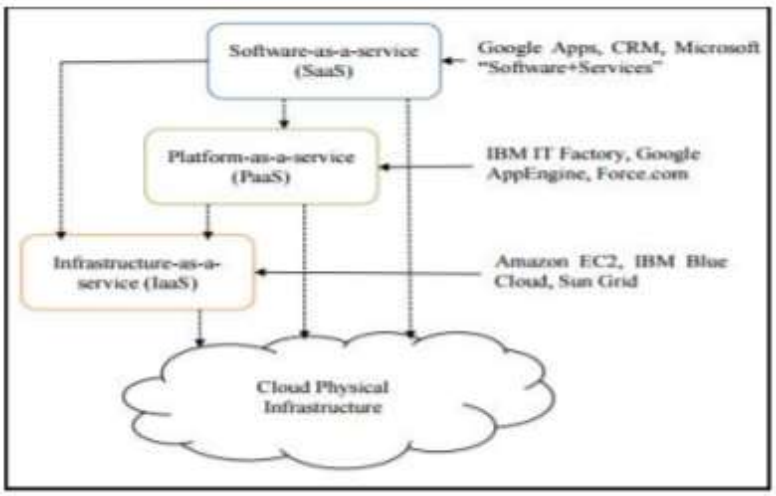

Figure 2: Cloud Services

Copyrighted Material

Google Docs as well as Zoho Suite are two instances of IaaS.

- Rather without having to worry about acquiring, licencing, or maintaining software, the SaaS providers install but also distribute it as needed for their customers [5]. Some of the applications in this list may be rented from service provider for a fee based on how much time or even resources the user uses. Users may access this programme using a web browser since it is hosted on the cloud. Instances of SaaS include, Salesforce.com, GoogleDocs and others.
- If you're looking for a way to build, deploy, run, and manage your apps in cloud with not having to worry about complexity of maintaining your own infrastructure, then PaaS is for you. In this paradigm, the user has access to the actual infrastructure of cloud as well as may choose the settings that are required to execute or deploy his application. Google App Engine as well as Amazon Web Service are two instances of PaaS.

3. CLOUD DEPLOYMENT MODELS

Cloud service providers may provide a variety of deployment methods, including the public, the private, the hybrid, as well as the community cloud [8].

- Because a large number of people may access and use a public cloud, it is less secure and more exposed to various dangers.
- A private cloud is one that is exclusively used by a single organisation and is the only accessible by that business. As a result, private clouds are more secure than the public ones.
- There are two types of hybrid cloud deployments: those that use both public as well as private clouds, and those that use either one or the other. In comparison to public cloud, this solution provides greater security and lower operating costs.
- As being such, community cloud is indeed a private cloud utilized by numerous businesses and isn't really a different deployment architecture.

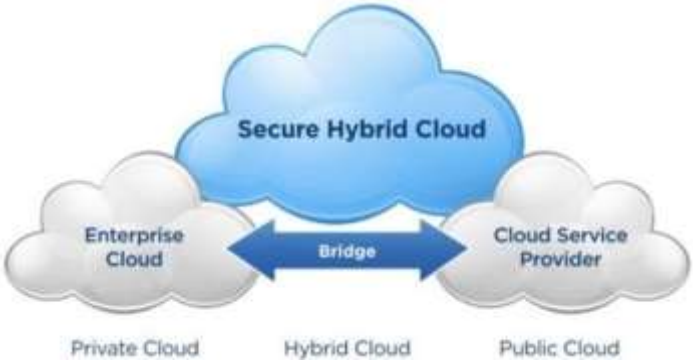

Figure:3 Cloud Models

Copyrighted Material

4. ATTACK AND CORRECTIVE RECTIFICATION WITHIN A CLOUD

4.1. SaaS layer attack:

Among SaaS customers, data security concerns such as data backup, the data access, and the data availability are indeed the most common complaints.

1. **DoS attacks**

Denial-of-service assault (DoS) was among the Cloud's most notable attacks. The hacker's main goal was to exhaust all of the user's personal information by sending out a large number of the request packets across the network..,[9,10]

2. **SQL injection attack:**

A malicious cryptogram or code was injected into network in the shape of legitimate input, with the goal of stealing all data about the victim's usage of the internet, such as their registered user, pin, credit card number, etc. That's when the hacker gets access towards the user's private information illegally. [11].

3. **Authentication attack:**

Weak usernames and passwords were to blame for the assaults on authentication. In just this authentication assault, which is a little out of control, the hacker pretends to become a user to mislead the system as well as get access they shouldn't have. [12].

4.2. PaaS layer attack:

The side channel and cross-site attacks were other names for this assault.

1. **Port Scanning Attack**

This was a well-known exploit wherein a hacker gains access to a portal URL, extracts data, and either destroys or misuses the data. [13].

2. **Metadata spoofing**

attack Here in which the attacker access the file and make some modifications or else delete some of the important operations [14].

3. **Man-in-the-browser**

Attack Here in which the attacker was stand between the sender and the receiver and can access the information [15].

Copyrighted Material

4. **Phishing / Spoofing attacks**

Phishing or the spoofing attacks will have an effect on both the server and users. Here the user can redirected to the spoofed web link and the attacker can access and get the personal information about the user [16].

4.3. IaaS layer attack

Attacks will occur often on such layer because virtualization administrator lacks a defence opening [17].

1) **Cross-virtual-machine attacks** Another name for this technique is side channel attack. While extracting as well as destroying some secondary data like power, volt, but also minutes, here is where user-confidential details may be found. [18].
2) **Virtual machine (VM)** rollback attack: Here, attacker has access to the passcode of virtual machines, thus he or she may take a picture of one and execute it without user's knowledge. The brute-force assault is used in this case. A component for controlling permissions, rollback, may be used by the attacker to alter user's ease of access or authorisation code [19].
3) **VM escape attack:** Attackers target downed guest operating systems or memory information throughout such sort of attack. Attackers have full control of guest operating system beyond this point. [20].

5. SECURITY ARCHITECTURES AND PROTOCOLS

In current history, a number of academics have come up with solutions for cloud security issues. A few of the security designs including models provided by professionals in the fields of availability of services, secrecy, including data integrity, such as proof of the data ownership, recoverability, dynamic audits, as well as data deduplication within single as well as multi-cloud systems, are included below. However, even though multi-cloud storage offers a high degree of security, certain means for verifying data integrity must be in place in the event that unauthorised modifications are made. When it comes to data integrity verification in the cloud computing, public auditing is perhaps the most popular solution. A user's data and also their requester's identification are kept hidden by such auditing procedures in order to preserve complete confidentiality. This may be done by implementing Evidence of Retrievability also represented as (PoR) techniques, which enable verifiers to figure out if the data block or even file is owned or not owned by a prover. [21][22][23].

[23] The PoR technique was created in 2003, and it attempts to guarantee the accessibility of files exchanged across several peer servers. To ensure the integrity of file, they advocated the use of the error-coding to file, as well as peer-to-peer file verification. Their technique assumes that each instance has its own MAC and therefore does not need a solitaire server's error correcting. The study's definition of verification method is also vague.

Copyrighted Material

6. CONCLUSION

Despite the fact that cloud computing security has been extensively explored, the goal of this article, for example, the review of literature within the field of the cloud computing security, has been met (Cloud fundamentals, issues as well as various security infrastructures). We discussed a variety of the cloud deployment techniques and cloud-based services. The issues which prevent most businesses from using cloud services, including as integrity, accessibility, and protection, are examined in depth. Research shows that multi-cloud designs are better equipped to deal with cloud computing challenges, and they've been a popular trend in recent years because of their capabilities. To sum up, we can assume that the multi-cloud systems are always in their early stages; they still have a long way to go before they can be considered secure enough to protect data as well as user privacy, as well as efficient enough to handle complex computations, communications, including dynamic operations inside an efficient manner.

REFERENCES

1. Gartner, “Gartner identifies the top 10 strategic technologies for 2011”, “web reference”: http:// www.gartner.com/it/page.jsp?id=1454221, “Last access date”: 02 Dec. 2016.
2. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.
3. Hassan, Qusay (2011). "Demystifying Cloud computing" (PDF). The Journal of Defense Software Engineering. CrossTalk. 2011 (Jan/Feb): 16–21. Retrieved 11 December 2014.
4. Peter Mell and Timothy Grance (September 2011). "The NIST definition of Cloud computing" (technical report), National Institute of Standards and Technology: U.S. Department of Commerce. doi:10.6028/NIST.SP.800-145. Special publication 800-145.
5. Hassan, Qusay (2011). "Demystifying Cloud computing" (PDF). The Journal of Defense Software Engineering. CrossTalk. 2011 (Jan/Feb): 16–21. Retrieved 11 December 2014.
6. Harold C. Lin, Shivnath Babu, Jeffrey S. Chase, Sujay S. Parekh, “Automated control in Cloud computing: Opportunities and Challenges”, Proc. of the 1st Workshop on Automated control for data centres and clouds, New York, NY, USA, pp. 13-18, 2009, ISBN: 978- 1-60558-585-7.
7. William Y. Chang, Hosame Abu-Amara, Jessica Feng Sanford, Transforming Enterprise Cloud Services, London: Springer, 2010, pp. 55-56.
8. E. Gorelik, “Cloud computing models,” 2013. [Online]. Available: http://web.mit.edu/smadnick/www/wp/2013-01.pdf. Accessed: Feb. 12, 2016.

Copyrighted Material

9. G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Computer Communications, vol. 107, pp. 30-48, 2017.
10. L. Alhenaki, A. Alwatban, B. Alamri, and N. Alarifi, "A Survey on the Security of Cloud Computing," in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019, pp. 1-7.
11. P. Deshpande, S. Sharma, S. K. Peddoju, and A. Abraham, "Security and service assurance issues in Cloud environment," International Journal of System Assurance Engineering and Management, vol. 9, pp. 194- 207, 2018.
12. A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," Journal of Network and Computer Applications, vol. 79, pp. 88-115, 2017.
13. N. Almasalmeh, F. Saidi, and Z. Trabelsi, "A Dendritic Cell Algorithm Based Approach for Malicious TCP Port Scanning Detection," in 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 2019, pp. 877-882.
14. R. Anitha, P. Pradeepan, P. Yogesh, and S. Mukherjee, "Data storage security in cloud using metadata," in 2nd International Conference on Machine Learning and Computer Science (IMLCS'2013), Kuala Lumpur (Malaysia), 2013, pp. 26-30.
15. A. Mallik, A. Ahsan, M. Shahadat, and J. Tsou, "Man-in-the-middle-attack: Understanding in simple words," International Journal of Data and Network Science, vol. 3, pp. 77-92, 2019.
16. V. S. P. P. C. Kumar and S. P. Rao, "Phishing attack detection," ed: Google Patents, 2019.
17. F. Mohammed and D. Uliyan, "A New Password Authentication Scheme Resistant against Shoulder Surfing Attack," 技術學刊, vol. 34, 2019.
18. S. Anwar, Z. Inayat, M. F. Zolkipli, J. M. Zain, A. Gani, N. B. Anuar, et al., "Cross-VM cache-based side channel attacks and proposed prevention mechanisms: A survey," Journal of Network and Computer Applications, vol. 93, pp. 259-279, 2017.
19. P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, "Intrusion detection techniques in cloud environment: A survey," Journal of Network and Computer Applications, vol. 77, pp. 18-47, 2017.
20. Y. Xia, Y. Liu, H. Chen, and B. Zang, "Defending against vm rollback attack," in IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN 2012), 2012, pp. 1-5
21. M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard. “A cooperative Internet backup scheme”, USENIX Annual Technical Conference, General Track 2003, pages 29—41, 2003.

Copyrighted Material

22. H. Shacham and B. Waters, "Compact proofs of retrievability," Advances in Cryptology-ASIACRYPT 2008, pp. 90–107, 2008.

23. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in Cloud computing," Computer Security–ESORICS 2009, pp. 355–370, 2009.

Copyrighted Material