International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

An Analysis of Cloud Computing Risk and Challenges

Shivam Dhoot[1], Himanshu Gupta[2]

AIIT, Amity University, Noida, India
shivam.dhoot[at]s.amity.edu
hgupta[at]amity.edu

Abstract: ***Cloud computing is a new paradigm that has quickly risen to the top of the research agenda due to its ability to lower computing costs. In today's world, it is the most fascinating and tempting technology that provides consumers with on-demand services over the internet. Since Cloud computing stores data and disseminated services in an open environment, security has become the most significant barrier to Cloud implementation. Even though Cloud Computing is promising and effective, data protection is a major concern since the data is not in the Cloud user's immediate vicinity. I described various Cloud Security Issues, Threats, Risks and Challenges.***

Keywords: Cloud Computing, Models, Security Challenges, Threats

1. Introduction

Cloud computing refers to the practise of storing and accessing data and programmes on remote servers over the internet rather than on the computer's hard drive or local server. Internet-based computing is another term for cloud computing [1].

Every day, we probably use a variety of cloud-based software. When we send a file to a colleague through the web, use a mobile app, download a picture, binge a Netflix movie, or play an online video game, you're using cloud solutions. Many of these resources are stored in the cloud and live somewhere in cyberspace. Holding the data on a laptop hard drive or a USB stick is very different from storing it on OneDrive, SharePoint, or an email server. It can be accessed from almost any computer that has access to the internet [2]. The architecture of cloud computing is shown in figure 1.

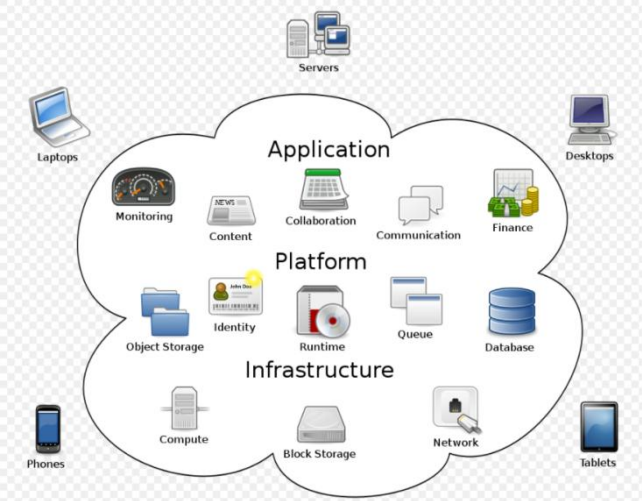

Figure 1: Architecture of Cloud Computing

The advantages of using cloud computing include:

- Reduced hardware and support cost,
- Accessibility all throughout the planet, and
- Flexibility and profoundly computerized measures wherein the client need not stress over ordinary concerns like software up-gradation.

2. Service Models in Cloud Computing

1) **Software-as-a-Service (SaaS):** Software-as-a-Service (SaaS) is otherwise called "on-demand software". It is programming in which the applications are facilitated by a cloud specialist organization. Clients can get to these applications with the assistance of a web association and an internet browser.Some examples of Software-as-a-Service is Google apps, Drop Box [3].
2) **Platform-as-a-Service (PaaS):** Platform as a Service (PaaS) gives a runtime climate. It permits developers to handily make, test, run, and send web applications [3]. You can buy these applications from a cloud specialist co-op on a compensation according to utilize premise and access them utilizing the Internet association. In PaaS, back-end versatility is overseen by the cloud specialist organization, so end clients don't have to stress over dealing with the framework.
3) **Infrastructure-as-a-Service (IaaS):** Infrastructure-as-a-service (IaaS) is otherwise called Hardware as a Service (HaaS). It is a processing foundation oversaw over the web. The principal benefit of utilizing IaaS is that it assists clients with staying away from the expense and intricacy of buying and dealing with the actual workers. Some of Some examples of Infrastructure-as-a-Service is Amazon Web Services (AWS), Microsoft Azure [3].

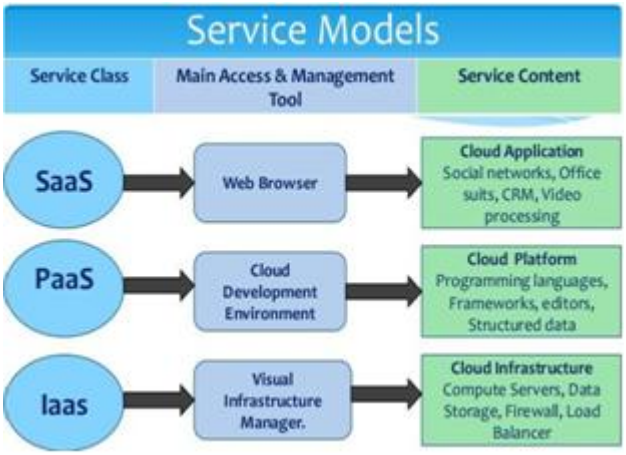

Figure 2: Service Models

3. Cloud Deployment Models

The Cloud Computing has four main deployment models which are-:

1) **Public Cloud:** Describe cloud computing within side the conventional sense, wherein outside third-party carriers who proportion assets and payments dynamically offer assets via net packages/net offerings via the Internet on a fine-grained self-provider foundation. The basis of self-computing. Compared with different cloud models, public clouds are much less stable due to the fact they boom overhead. Ensure that each package and facts accessed within side the public cloud have now no longer been maliciously attacked [4].
2) **Private Cloud:** Private clouds are allotted structures that work on a non-public infrastructure and imparting the customers with dynamic provisioning of computing resources. Instead of a pay-as-you-go version as in public clouds, there can be different schemes in that don't forget the use of the cloud and proportionally billing the one-of-a-kind departments or sections of an enterprise [1].
3) **Hybrid Cloud:** Hybrid Cloud integrate public cloud with non-public clouds.They are designed to permit the 2 systems to have interaction seamlessly, with information and applications shifting easily from one to the other. It's the appropriate solution for an enterprise or employer that wishes a touch little bit of each option, normally structured upon enterprise and size [5].
4) **Commuity Cloud:** Community Cloud is a collaborative, multi-occupant stage utilized by a few particular associations to have similar applications. The clients are normally working inside a similar industry or field and offer regular worries as far as security, consistency, and execution. Generally, a community cloud is a private cloud that capacities similar to a public cloud. The actual stage is overseen secretly, either in a data centre or on-premises. Approved clients are then portioned inside that climate. These arrangements are normally utilized by government offices, medical care associations, monetary administrations firms, and other expert networks [5].

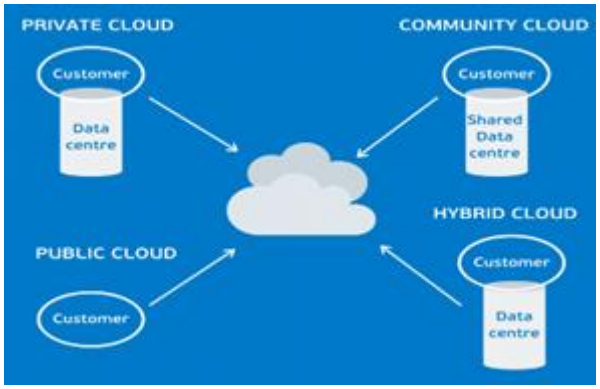

Figure 3: Cloud Deployment Models

4. Risk and Challenges

As we realize that there are two principal sorts of Cloud Computing, for example, Public Cloud and Private Cloud, so we talk about security issues for both.

Security issues in Public Cloud [6]

1) Three essential necessities of security: privacy, integrity and accessibility are needed to ensure information all through its lifecycle. Information should be secured during the different phases of creation, sharing, chronicling, handling and so forth. Nonetheless, circumstances become more convoluted if there should be an occurrence of a public cloud where we don't have any command over the specialist organization's security practices.
2) If there should be an occurrence of a public cloud, a similar framework is divided among various occupants and the odds of information spillage between these inhabitants are high. However, the vast majority of the specialist organizations run a multitenant foundation. Appropriate examinations at the hour of picking the specialist co-op should be done to stay away from any such danger.
3) In the event that a Cloud Service Provider utilizes an outsider merchant to give its cloud administrations, it ought to be guaranteed what administration level arrangements they have in the middle just as what are the emergency courses of action if there should be an occurrence of the breakdown of the outsider framework.
4) Appropriate Service-Level Agreement (SLAs) characterizing the security prerequisites, for example, what level of encryption information ought to go through, when it is sent over the internet and what are the punishments in the event that the specialist organization neglects to do as such.

Security issues in Private Cloud [6]

1) Virtualization methods are very famous in private clouds. In such a situation, dangers to the hypervisor ought to be deliberately broken down. There have been occurrences when a visitor working framework has had the option to run measures on another visitor VMs or host.
2) The host working framework ought to be liberated from such a malware danger and observed to keep away from any such danger. Also, visitor virtual machines ought not have the option to speak with the host working

framework straightforwardly. There ought to be devoted actual interfaces for speaking with the host.

3) While we discuss standard web security, we likewise need to have a security strategy set up to protect the framework from the assaults beginning inside the association. This fundamental point is passed up the majority of the events, stress is for the most part upon the web security. Legitimate security rules across the different divisions should exist and control ought to be executed according to the prerequisites.

Some other issues related to cloud security are mentioned below-:

1) **Legal/Compliance Issue:** With expanding unofficial laws relating to information assurance like General Data Protection Regulation(GDPR) and Health Insurance Portability and Accountability Act(HIPAA), remaining agreeable is getting more unpredictable. Attributable to the huge scope of openness of information on the cloud climate, it very well may be hard for organizations to monitor who can get to the data. Organizations ought to consistently endeavour to stay agreeable with laws and industry guidelines to try not to confront heavy fines and reputational harm as a result of an effective security occurrence [7].
2) **Third-Party Control:** The significant security challenge is the outsider issue, that is, the proprietor of the information has no control over their information handling. The greatest chance for the Information Technology (IT) branch of the association utilizing distributed computing will be diminished control even as they are being entrusted to bear expanded duty regarding the secrecy furthermore, consistency of processing practices in the association [6].
3) **Data Privacy:** Information protection or data security is a part of information security worried about the appropriate treatment of information – consent, notice, and administrative commitments. Your information is your information. You don't need anyone to get to it except if you permit them to.
4) **Multiple Stakeholders:** In a distributed computing model, there are various partners included: cloud supplier, specialist organization, and client. Every partner has their own security the board frameworks/measures and their own assumptions (necessities) and abilities (conveyed) from/to different partners. This additionally prompts making issues.

5. Threats in Cloud Computing

There are various security issues for cloud computing as it envelops numerous innovations including networks, databases, working frameworks, virtualization, transaction management, load adjusting, simultaneousness control and memory management [4].It is important for associations to know about digital dangers. As indicated by the Cloud Security Alliance report, here are the top dangers to distributed computing:

1) **Data Breaches-:** It can be the main goal of an attack through which sensitive information such as health, financial, personal identity, intellectual and other related information is viewed, stolen or used by an unauthorised user.
2) **Insufficient identity, Credential and Access Management-:**Security dangers may happen because of deficient assurance of the certifications. An unapproved client might read, alter and erase the information or release malicious software.
3) **Insecure Interfaces and APIs:** Cloud specialist co-ops uncover a bunch of programming UIs or application programming interfaces (APIs) that associations use to oversee and connect with the cloud administrations. Additionally, clients and outsider clients regularly offer administrations to their clients through these interfaces [8].An unapproved client may access and re-utilize these APIs or passwords. They may send content, get approvals and logging capabilities.
4) **Traffic Hijacking:** Record or administration seizing should be possible to obtain entrance and misuse exceptionally special records [8]. Assault techniques like extortion, phishing, and abuse of software weakness are completed for the most part utilizing the taken passwords.
5) **Malicious Insider:** A malicious insider can get to delicate information of the framework chairman or may even oversee the cloud administrations at more noteworthy levels with practically zero danger of recognition. A malicious insider may influence an association through brand harm, monetary effect and productivity loss [8].

Some of the top threats are described above.

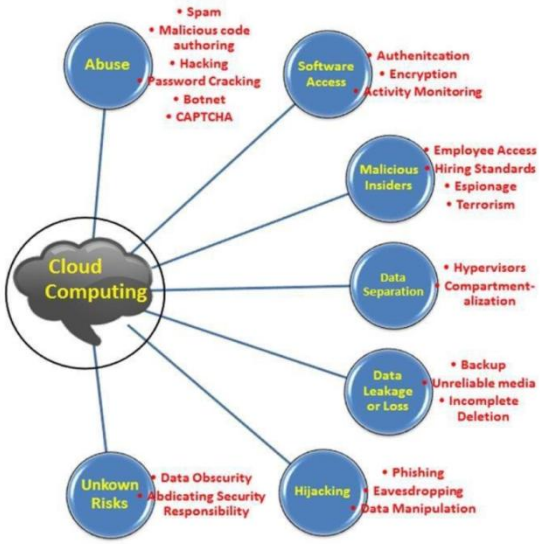

Figure 4: Several other threats to computing

6. Proposed Solutions

Cloud suppliers should address data security and protection chances related to sending data into any distributed computing climate. The following are some proposed solutions for the issues talked about.

1) Cloud providers ought to guarantee that information in the cloud environment is sealed, ensured through encryption at the piece level. Communication between the client and the supplier's work is secure, hence keeping away from the danger of any man-in-the-centre assaults to access the encryption keys.

2) Cloud provider should utilize industry-standard AES encryption to make information unintelligible and unusable to those without the encryption key.Data theft, openness to unapproved meetings, and information seizure by a legitimate summons are all greatly reduced by making the information useless to deliver.
3) Providers ought to give an exceptional arrangement-based way to deal with key administration and information access that permits clients to decide precisely which server gets access to secure data.
4) Secure the entirety of your cloud clients with multi-factor authentication (MFA) to guarantee that a solitary approved workforce can sign in to your cloud applications and access that touchy information in your on-or off-premise environment [9]. MFA is one of the least expensive yet best security controls to hold would-be software back from getting to your cloud applications.
5) Relegating access control not just keeps a representative from inadvertently altering data that the individual in question isn't approved to get to, yet additionally shields you from hackers who have stolenan employee's certification. It ought to likewise be noticed that numerous administrative consistency norms, like HIPAA, FINRA and numerous others, require these sorts of safety efforts [9].

7. Conclusion

Cloud computing is another innovation that gives numerous advantages like storage capacity, cost depletion, time, processing power and execution powerful innovation. In any case, it has its own security issue that compromises the association to embrace cloud technology.

As Individuals, government and nongovernmental association, little and huge scope undertakings make arrangements to send their information and different applications in private, local area and public cloud environments, new security moves should be tended to. Ideal cloud security practices ought to incorporate encryption of delicate information utilized by cloud-based virtual machines; centralized key administration that permits the client (and not the cloud provider) to control cloud information, and guaranteeing that cloud information is available as indicated by setting up big business arrangements. This paper examines the advantage of utilizing cloud computing, the danger and difficulties of this new innovation and the danger that are arising which assault the secrecy and weakness of the data in the cloud. In the end proposed answer for shielding data in both private, public, local area cloud administrations were referred to.

References

[1] Y. Sharma, H. Gupta and S. K. Khatri, "A Security Model for the Enhancement of Data Privacy in Cloud Computing," 2019 Amity International Conference on Artificial Intelligence (AICAI), 2019, pp. 898-902, doi: 10.1109/AICAI.2019.8701398.
[2] Cloud Security Alliance (CSA) 2014. Big Data Working Group Big Data Taxonomy, September 14.
[3] H. Gupta et al., "Impact of Side Channel Attack in Information Security," 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2019, pp. 291-295, doi: 10.1109/ICCIKE47802.2019.9004435.
[4] Usman Namadi Inuwa Int. Journal of Engineering Research and Applications ISSN: 2248-9622, Vol. 5, Issue 12, (Part – 4) December 2015, pp.05
[5] G. O. Boussi and H. Gupta, "A Proposed Framework for Controlling Cyber- Crime," 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2020, pp. 1060-1063, doi: 10.1109/ICRITO48877.2020.9197975.
[6] Imran, Faisal & Yunfei, Yin & Ikram, Mohammad. (2019). CLOUD COMPUTING SECURITY ISSUES AND THREATS IN BUSINESS ENVIRONMENT.
[7] G. Himanshu and K. Desire Afewou, "A trust model for security and privacy in cloud services," 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2017, pp. 443-450, doi: 10.1109/ICRITO.2017.8342468.
[8] Srivastava, Priyanshu & Khan, Rizwan. (2018). A Review Paper on Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering. 8. 17. 10.23956/ijarcsse.v8i6.711.
[9] Prasad, M.Rajendra & Naik, R Lakshman & V, Dr. Bapuji. (2013). Cloud Computing : Research Issues and Implications. International Journal of Cloud Computing and Services Science. 2. 134-140. 10.11591/closer.v2i2.1963.