Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 10, October 2019

CLOUD COMPUTING PROTECTION ISSUES

Mr. Kidiyappa Maddennavar
Faculty of Engineering and Technology
Jain (Deemed-to-be University), Ramnagar District, Karnataka - 562112
Email Id: m.kidiyappa@jainuniversity.ac.in

Abstract

Cloud computing is considered to have many prospective benefits and many business systems and knowledge migration to the public cloud or hybrid cloud. But with respect to others Business-critical applications, organizations, particularly large organizations, Businesses wouldn't transfer them to the cloud at all. The Scale of the Competition shared cloud computing is still far behind the one that was planned. Cloud computing protection, from the perspective of consumers, Concerns, especially issues of data security and protection of privacy, the key inhibitor of cloud computing adoption is still the primary inhibitor of Services. In this paper we discuss cloud computing security issues and data security and privacy protection issues.

Keywords: *Cloud Computing, Challenges, Data Security, Protection, Security Issues, Hybrid cloud.*

I. INTRODUCTION

Cloud Computing allows for ubiquitous, simple, convenient, network access to a common pool of configurable computing resources on demand (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned with minimal management effort or operation, and published interaction between providers [1]. As a technological paradigm, Cloud Computing appears as a distribution architecture and its main aim is to provide safe, rapid, convenient data Net computing service and storage, for all computing resources as services visualized and delivered over the Internet [2]. The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing [3].

From initial construction of ideas to current actual implementation, Cloud computing is gradually becoming more mature. Nowadays, however, many organizations, particularly small and medium enterprises, Increasingly, (SMB) businesses are recognizing the advantages of Putting into the cloud their applications and results [4]. Adoption of Cloud computing can lead to improvements in productivity and Development and implementation effectiveness and cost savings. For the procurement and repair of facilities [5].

In the cloud, traditional security concerns are still present. Environments for computing. But as business boundaries have limits, traditional protection frameworks are applied to the cloud and are no longer suitable for cloud applications and data [6]. Owing to the Cloud, cloud, transparent and multi-tenant characteristics computing is bringing tremendous impact on knowledge:

1. Because of complex scalability, abstraction of the operation, and Cloud computing models' position transparency characteristics, all there are no forms of applications and cloud platform data boundaries for fixed infrastructure and defence. In the case of It's hard to isolate a specific physical breach of security, a resource that has or has been compromised by a threat [7].

2. According to the models for cloud service delivery, computing, cloud-based resource resources, may be owned by different providers. Because a conflict of interest occurs, it is difficult to enforce a single safety measure;
3. As the cloud's transparency and virtualized sharing multi-tenant tools, user data can be accessed by other users Users that are illegal.
4. As the platform of the cloud has to deal with huge Storing and providing quick access to information, cloud protection the need for large data must be satisfied by measures production methods [8].

This paper describes data security and privacy protection issues in cloud. This essay is structured as follows: gives a brief overview of what exactly cloud computing the safety-related concerns are. Talks about data protection problems associated with cloud computing and data security both phases of the data life cycle. Displays the present Data security solutions and privacy protection solutions.

II. DISCUSSION

1. CLOUD COMPUTING SECURITY ISSUES:-

A. Cloud Computing Security: Protection of Cloud Computing as "Cloud Security" The protection of computing (sometimes referred to simply as "cloud" Defense") is an emerging computer security sub-domain, the security of the network, and, more generally, information security. It a wide variety of laws, technology and controls are referred to deploy to secure information, applications and the related information Cloud computing infrastructure. Note the Cloud Computing Security is not cloud-based security software, as stated here. Cloud-based antivirus products, anti-spam, anti-DDoS, And so on, etc.

B. *Security Issues Associated with the Cloud:* There are several cloud-related security concerns, computing and it's possible to group them into any number of the Proportions. Before making a cloud pick. Users should ask the suppliers for seven specific safety suppliers. Issues:

privileged user access, compliance with regulations, data Place, segregation of data, recovery, support for investigations, and Viability in the long run [9].

2. DATA SECURITY AND PRIVACY PROTECTION ISSUES

Content for cloud data security and privacy protection comparable to conventional data protection and privacy, it is protecting. In any stage of data life, it is also involved. But because of transparency and a function of multi-tenant the cloud, data security content, and protection of privacy cloud.

3. Data Life Cycle

The data life cycle refers to the entire generational process. And get the data deleted. The life cycle of data is divided into seven phases.

4. Data Generation

Data generation is involved in the ownership of knowledge. Inside the traditional IT climate, typically owned by users or organizations Info, and manage it. But if data is to be moved into the cloud, how to preserve data ownership should be considered. Data proprietors are entitled to personal private details Understand what sensitive information is collected, and in some Instances to halt the collection and use of personal data [10].

5. Transfer

Typically, data transmission within the business borders does not require encryption, or it simply requires simple data. Measure of Encryption. For business-wide data transmission the limits of confidentiality and honesty of data should be both ensured to avoid data from being tapped and retrieved Manipulated by unauthorized users. In other terms, it is just the Encrypting data is not enough? There is also a need for data integrity to be guaranteed. It should also ensure that transport protocols are regulated by providing both privacy and honesty [11].

6. Use

Using a simple storage service for static data, such as Data encryption for Amazon S3 is feasible. For the static, however, Data in the PaaS or SaaS model used by cloud-based applications, Data encryption is not feasible in certain circumstances. Since there is data Encryption can lead to indexing and query issues, Generally, static information used by cloud-based applications is not and encryption. Not only in the cloud, but even in conventional IT, the setting, the information being processed, is almost not encrypted for Any software with which to work. Because of the multi-tenant functionality of Cloud computing models store the data processed by cloud-based applications along with data from other applications.

7. Share

The exchange of data extends the spectrum of data and uses making data permissions more difficult. The proprietors of the data will enable one party to have access to the data and, in turn, the party will Share the data further without the permission of another party without the consent of Owners of data. Thus, during data sharing, in particular, if shared with a third party, the owners of the data need to consider if the third party is continuing to protect the Initial steps of safety and limits on use.

8. Storage

The data stored in cloud storage is identical to the information stored in cloud storage. Three components must be considered and processed in other locations. The security of information: confidentiality, honesty, integrity and availability.

III. CONCLUSION

Privacy security issues are the exchange of data though personal information security. The typical mechanisms that Privacy security is required by e-commerce systems that store data. Credit cards and health care programmes with information about health. The power to regulate what data to disclose and who can access information over the Internet has become an increasingly important issue. Concern. Such issues include whether sensitive information is personal. Third parties may store or read them without permission, or without consent. Whether third parties are able to monitor websites that someone has seen. Visited. Another issue is if the websites accessed are collect, store, and probably exchange personal data on users. In the cloud world, the secret to privacy security. The strict separation of sensitive information from non-sensitive information. The encryption of confidential elements is accompanied by security and privacy. For issues relating to data security and protection of privacy, the separation of confidential data and data is a key challenge. Controlling access. Our aim is to design a series of unified Frameworks of identity management and privacy security through Services for cloud computing or software.

IV. REFERENCES

[1] M. A. Vouk, “Cloud computing - Issues, research and implementations,” 2008, doi: 10.1109/ITI.2008.4588381.

[2] D. C. Chou, “Cloud computing risk and audit issues,” *Comput. Stand. Interfaces*, 2015, doi: 10.1016/j.csi.2015.06.005.

[3] A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey,” *Journal of Network and Computer Applications*. 2017, doi: 10.1016/j.jnca.2016.11.027.

[4] Q. Zhang, L. Cheng, and R. Boutaba, “Cloud computing: State-of-the-art and research

challenges," *J. Internet Serv. Appl.*, 2010, doi: 10.1007/s13174-010-0007-6.

[5] B. R. Kandukuri, P. V. Ramakrishna, and A. Rakshit, "Cloud security issues," 2009, doi: 10.1109/SCC.2009.84.

[6] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," 2012, doi: 10.1109/ICCSEE.2012.193.

[7] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing - The business perspective," *Decis. Support Syst.*, 2011, doi: 10.1016/j.dss.2010.12.006.

[8] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On technical security issues in cloud computing," 2009, doi: 10.1109/CLOUD.2009.60.

[9] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," *Futur. Gener. Comput. Syst.*, 2013, doi: 10.1016/j.future.2012.05.023.

[10] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*. 2011, doi: 10.1016/j.jnca.2010.07.006.

[11] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, 2012, doi: 10.1016/j.future.2010.12.006.