Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2017, 4(12):951-954

Review Article ISSN: 2394 - 658X

A Review Paper on Data Document and Service-related Security Issues in Cloud Computing

Mr. Chintal Patel[1] and Dr. Amit Sinhal[2]

[1]*Research Scholar, Department of CSE*
Sri Satya Sai University of Technology & Medical Sciences, Sehore, M.P., India.
smilingchintal@gmail.com
[2]*Professor, Department of CSE*
JK Lakshmipat University, Jaipur, Rajasthan, India
sinhal.amit@gmail.com

ABSTRACT

Cloud computing now a days become a very prominent field in all the area like engineering, Big Data Analytics, health care industry, Data storage etc. cloud computing is the way to enlarge the capabilities and capacity of company or institute without investing fund for training and infrastructure. Now a day's cloud computing is very important and emerging area of research because it reduces the cost that are associated with computing. The cloud computing postulation many of the services and resources online without installing any software. In the field of cloud computing technology, the main and foremost concern is reliability and security during Data upload on the server. On cloud server the incredible amount of data is available from different communities and security of data is very important and challenging concern in the field of cloud computing. In this paper we will discuss some of the technical issues and security concern related to the cloud computing.

Keywords: cloud computing, Data security, Multi-clouds, computing, Deployment models Big data Analytics

1. INTRODUCTION

Cloud is very important field in the field of information technology. CC is a technology that provides services resources and storage virtually through internet. Cloud computing provides facility to share resources, devices and storage sharing. Cloud computing technology expand the information technology proficiency by enlarging the capacity and add more abilities dynamically without investing large amount of money on expensive infrastructure, purchasing and licensing new software, or providing training to employees. Some of the services delivered by cloud computing is storage service, database management system, networking services, servers and software and many more over the internet platform (cloud).

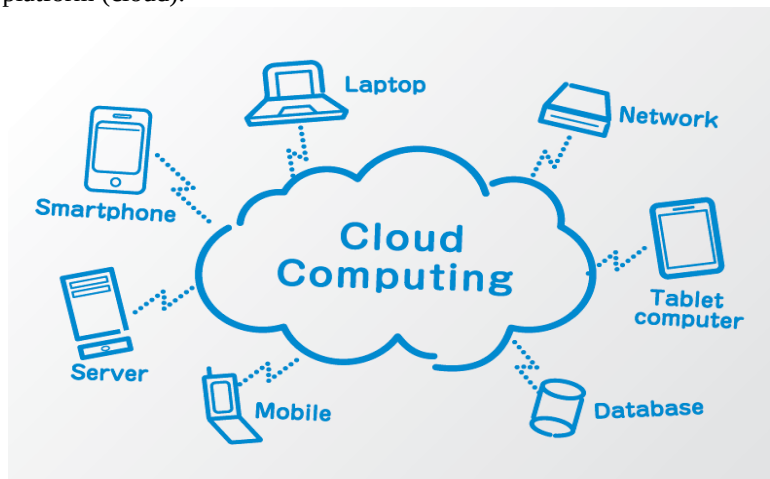

Fig. 1 Services provided by cloud computing

Cloud storage offers people and companies the ability to save on costs, enable higher productivity, speed, reliability, efficiency and protection for a variety of reasons [11]. The name of cloud computing is that accessed knowledge can be found in cloud or a simulated environment remotely. Cloud computing provides trouble-free and simple environment that is easily accessible online portal by any of the user and can take benefit of the services. Some of the Cloud service Suppliers are aws (amazonweb services), international Business Machine cloud (IBM cloud), terremark, joyent, rackspace, google cloud platform, and VMware. All the services provider provides services on the basics of demand or request of the user/ client.

Fig. 2 Cloud Service Providers

In today's area many of peoples are using cloud computing services rather than on- premises datacentres just because there are many of the advantages to use cloud computing services over on-premises datacentre. Some of the benefits are low cost, scalability, fast speed, high productivity, more reliable and security.

1.1 Categories of cloud computing:

Cloud computing is divided into three Categories.

1. **Public cloud:** Public cloud computing is the type of cloud computing that is owed and run by the other supplier (third-party) that is cloud service provider. The services and resources delivered by public cloud is software, servers and storage over the cloud.
2. **Private cloud:** Private cloud computing is the type of cloud computing that is solely owed and used inside a single organisation or business or company. The private cloud is installed and located in company.
3. **Hybrid Cloud:** hybrid cloud is the coalescence of private and public clouds. It is a computing technique that combines an on-premises data centres that is private cloud with at hird-party service provider that are public cloud.

Fig. 3 Categories of cloud computing

1.2 Types of cloud computing services:

There are three types of computing services are available that is software as services, platform as service and infrastructure as service.

1. **SaaS (Software as a Service):** SaaS is one of the model, in this all the services like software applications is hosted as service on web and all the client and end user access that software using web browser.
2. **PaaS (Platform as a Service):** PaaS is another model, in this client or end user originate, evaluate and upload applications using some tools and service provider. All the tools and libraries were hosted or given by cloud service provider.

3. **IaaS (Infrastructure as a Service):**IaaS is last model, this model is responsible or services related to infrastructure like storage, hard disk network and server etc.All the maintenance related work is responsibility of service provider.

2. LITERATURE REVIEW

Eman M. Mohamed (2012) et. al reviewed issues related to cloud services. The next wave of IT Enterprises is cloud computing [2]. Data security issues arise because all consumer and device data reside in provider premises. In cloud storage, both data and applications are not contained in full on the user's machine. Clouds usually have a single protection model, although certain clients have varying requirements. This can be solved by any cloud provider by using encryption algorithms to encrypt the data. This paper explores the central issue of data protection in the cloud. Eman M. Mohamed (2013) et. al proposed a data security model that provides a default single gateway as a platform [3]. This model is used for securing sensitive and confidential user data across all the cloud application. This model performs encryption on sensitive and confidential data before sending that data to cloud storage. If any of the unauthorized user or person try to access that data than that person is able to see only encrypted data. And if supposes authorized person wants to access that data this model will decrypt that data for use. This model contains powerful and rapid encryption algorithm and many more security tools. The main focus of this paper is securing the data on cloud. Author analysed all the data confidentiality and security issues that is require for utilizing cloud computing from data life-cycle. Author proposed data management frameworks for classification as well as provide risk management framework. Mohiuddin Ahmed (2012) et. al surveyed some of cloud computing related issue and new advanced research area [5]. This paper provides an advanced analysis based on the philosophy of cloud infrastructure and most up-to-date studies. R. Velumadhava Raoa (2015) et. al discussed some of data-related protection issues. Security provision is a primary consideration when data are passed over a channel to the remote server (internet) [6]. Security issues must be resolved first before introducing cloud infrastructure in an enterprise. This paper author emphasizes data-related protection issues and strategies in a cloud-based setting. Hussam Alddin Shihab Ahmed (2016) et.al audits and help to resolve the essential and important issues of cloud-computing framework [7]. They portray all the information security, confidentiality of knowledge and safety for cloud privacy. Akhil Behl (2011)examines the current safety approaches to securing and safeguarding cloud networks and software [8]. They also address some of the main research obstacles in introducing modern cloud-based security technologies that provide proactive safety for diverse and ever- dynamic cloud infrastructures. Vassilka Tchifilionova (2011) discussed about protection and safety concerns and a standard legislative structure lack [9]. Cloud infrastructure – a modern model for information technology users, the future of the economies of scale, the illusion of limitless infrastructure access. Neelu Sinha (2014) et. al discussed the fundamentals and a short history of cloud infrastructure and its advantages and applications in architecture [12]. Finally, they provide an overview into cloud infrastructure problems and obstacles. Valentina Casola (2013) et. al presents a new computer paradigm, cloud system, capable of fully integrating the cloud and grid [14]. In this paper three-layer design is presented, and the security problems are explored and the approach proposed focused on fine-grained frameworks for access control and identity federations, which allow collaboration and interoperability between untrusty cloud services.

3. RISK AND SECURITY CONCERN IN SINGLE CLOUD

3.1 Data Breach through Hacked Interfaces and Insecure APIs

Data Breach is the process in which the confidential data is viewed, accessed, or stolen by the third party without any authorization, so organization's data is hacked by the hackers. When we are providing few services to public domain through API (Application Programming Interface), so we have to make sure of secure APIs.

3.2 Vendor lock-in

While we are using cloud services of any vendor from past several years and due to some up gradation or better cost we are planning to move or transferring the same to another vendor or cloud providers, we have to face many difficulties due to their different versions of platforms. So, in this way we can say that While Using Computing Vendor lock-in or vendor dependency is a security risk.

3.3 Requirements of well-trained IT Staff

Migration, Integration, and operation of Cloud Services are more complex for any organization. We need experts for the same who have extra knowledge and ability to integrate and manage the data over the cloud.

3.4 Meltdown & Spectre

These programs capture data from the user's computer system and mobile system. Generally, programs are not allowed to read the data of other programs. Meltdown & Spectre allows these programs to steal the data in the memory of other running programs such as your personal photos, email, instant messages and documents even though your passwords which are stored in your browser.

3.5 Denial of Service (DoS) attacks

In a denial-of-service (DoS) attack, a Server or network is targeted so that the hacker can shut it down so as to deprive the user (ie employees, members, or account holders) of the facilities offered by that Server. These attacks target the data servers of high-profile organizations such as banking sectors, ecommerce companies and government organizations. However, DoS attacks usually do not involve the theft or loss of important information or other property.

3.6 Account Hacking

This is a very critical risk in cloud computing. Through this process, hackers steals the data of the users or organization's cloud account, whether it is a bank account, email account and other social media accounts, and then these stolen accounts are used to carry out unauthorized activities.

4. CONCLUSION

In this paper by reviewing many of the research related to cloud computing services we came to know and generalize that security is very major and important concern because of confidentiality of data stored over the cloud. For protecting the data many of encryption algorithms are available with the help of cryptographic techniques. So, to use these encryption technologies to protect the data is one of the solutions. Other major solution is use of multi-cloud technology. Multi-cloud is facility to use of multiple cloud services that are provided by different services provider inside single network architecture. Multi- cloud provides best services of every platform and lower risk of down time, vendor lock-in and security. Multi- cloud provides best services and security to client or end user.

REFERENCES

[1] Eman M. Mohamed, Hatem S. Abdelkader and Sherif EI-Etriby (2012), “Enhanced Data Security Model for Cloud Computing”, The 8th International Conference on INFOrmatics and Systems (INFOS2012), CC-13-17.

[2] Meslhy, Eman, Abdelkader, Hatem & Eletriby, Sherif. (2013), “Data Security Model for Cloud Computing”, Journal of Communication and Computer 10 1047-1062. 10. 1047-1062. 10.13140/2.1.2064.4489.

[3] Mohiuddin Ahmed, Abu Sina Md. Raju Chowdhury, Mustaq Ahmed and Md. Mahmudul Hasan Rafee (2012), “An Advanced Survey on Cloud Computing and State-of-the-art Research Issues”, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, ISSN (Online): 1694-0814.

[4] R. Velumadhava Rao, K. Selvamani (2015). Data Security Challenges and Its Solutions in Cloud Computing. Procedia Computer Science. 48. 204-209. 10.1016/j.procs.2015.04.171.

[5] Alhadawi Hussam & Zolkipli Mohamad. (2016), “Data security issues in cloud computing: review”, International Journal of Software Engineering & Computer Systems (IJSECS). 2. 2289-8522. 10.15282/ijsecs.2.2016.5.0016.

[6] Akhil Behl (2011), "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," World Congress on Information and Communication Technologies, Mumbai, India, 2011, pp. 217-222, doi: 10.1109/WICT.2011.6141247.

[7] Vassilka Tchifilionova (2011), “Security and Privacy Implications of Cloud Computing – Lost in the Cloud”, Open Research Problems in Network Security, Volume 6555, ISBN: 978-3-642-19227-2.

[8] M. Irfan, M. Usman, Y. Zhuang and S. Fong (2015), "A Critical Review of Security Threats in Cloud Computing," 3rd International Symposium on Computational and Business Intelligence (ISCBI), Bali, Indonesia, 2015, pp. 105-111, doi: 10.1109/ISCBI.2015.26.

[9] N. Sinha and L. Khreisat (2014), "Cloud computing security, data, and performance issues," 2014 23rd Wireless and Optical Communication Conference (WOCC), Newark, NJ, USA, pp. 1-6, doi: 10.1109/WOCC.2014.6839924.

[10] Ahmed, Monjur& Hossain, Mohammad (2014), “Cloud Computing and Security Issues in the Cloud. International Journal of Network Security & Its Applications”. 6. 25-36. 10.5121/ijnsa.2014.6103.

[11] Valentina Casola, Antonio Cuomo, Massimiliano Rak and Umberto Villano. (2013), “The Cloud Grid approach: Security analysis and performance evaluation”, Future Generation Computer Systems. 29. 387-401. 10.1016/j.future.2011.08.008.