DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4355

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SECURITY AND PRIVACY APPROACH OF CLOUD COMPUTING ENVIRONMENT

Jahangeer Qadiree
Department of Information Technology,
Aisect University, Institute of Science and Technology,
Raisen, MP. India

Neha Prasad
Department of Computer Science & Engineering,
Sagar Institute of Science & Technology,
Bhopal, MP, India

Dr. Pratima Gautam
Dean of Information Technology Department,
Aisect University, Institute of Science and Technology,
Raisen, MP, India

Abstract: Cloud computing model are obtaining ubiquitous authorization due to the heterogeneous convenience they provide. Although, the security & privacy problems are the main considerable encumbrance holding back the universal adoption of this new emerging technology. Various researches are concentrated on enhancing the security on Software as well as Hardware levels on the cloud. But these interpretations do not mainly furnish the complete security way and therefore the data security compute (measure) are still kept under the access control of service provider. Trusted Computing is another research concept. In actuality, these furnish a set of tools controlled by the third party technologies to secure the Virtual Machines from the cloud computing providers. These approaches provides the tools to its consumers to assess and monitor the aspects of security their data, they don't allocate the cloud consumers with high control capability. While as the new emerging DCS approach aims to provide the security of data owners of their data. But the DCS approach concept is elucidate in many ways and there is not a standardized framework of cloud computing environment model for applying this approach.

Keywords: Data Centric Security, Security Issue, Data Security.

1. INTRODUCTION

Cloud Computing is an internet based technology of computing, where the software, information as well as shared resources are provided to the cloud users on demand services as per the user requirements. Cloud computing is the most emerging technology, but the security as well as the privacy of data are the main issues of cloud computing. Cloud computing, one of the emerged and most powerful system used by both developers as well as users provides the environment development and the resources allocation to its users when need. Cloud resources are shared widely and accessed. The availability of cloud resources results vulnerable. Because when the unauthorized user gets access to the data may change the original data that causes the major security risk [1]..

2. CLOUD COMPUTING SECURITY TRENDS & DIRECTIONS

The fastest growing technology of Cloud computing environment is facing numerous hindrances those cannot be neglected directly by the traditional techniques. An appropriate technique should be adapted for the specific features of new computing paradigm [1]. There are numerous research directions available to address the cloud problem as per the type of problem. There is also a possibility when an untrusted provider of cloud computing can control the licit way by handling the cloud users' request operations to their advantage. So by protecting the data, mainly its integrity as well as the privacy from the both of providers and the external intruders will be expected to the bold result in the cloud security architecture that will stimulate widely adaptation of the cloud computing services [2]. The various security trends of cloud computing environment are shown in the figure 1.1.

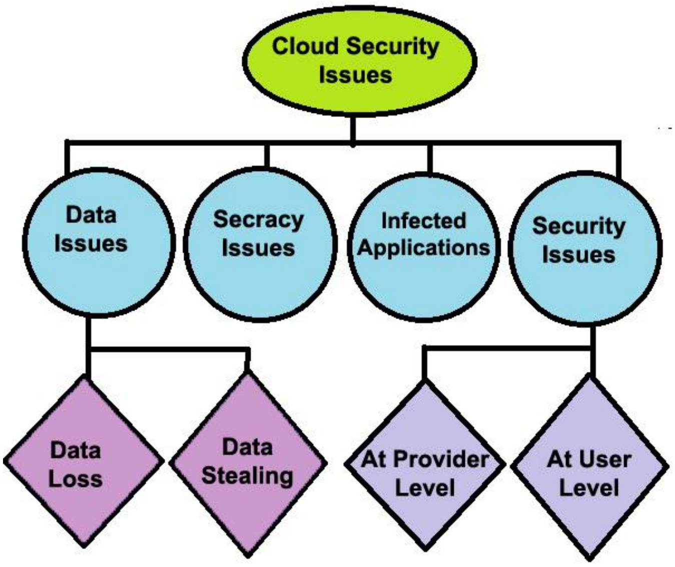

Figure 1.1 Security issues of Cloud Computing.

3. PRESERVING PRIVACY OF DATA FROM CLOUD PROVIDERS

The integrity as well as the privacy factor of various cloud based applications is the main important requirements. The customers of cloud based computing are not only troubled of their data regarding the integrity and privacy from the unauthorized intruders, as they are also worried about the unrealized curious cloud providers [3]. In the cloud computing environment, the data of customer's are outsourced to the trusted or un-trusted cloud providers [4]. The un-trusted term is used to describe that the providers of cloud can't be fully believed. However they may not change the customers data instead they may compromise the user's data privacy either they may alter the standards for their benefits. The cloud computing service provider's may be contemplate as a honest by providing their valid users the security features related their data as well as process the authorized user's quires and retrieves the true results [5] . The encrypted data on cloud are totally secured from the users who do not have the valid credentials to access, even if they access the data can't be beneficial untill decryption [6].

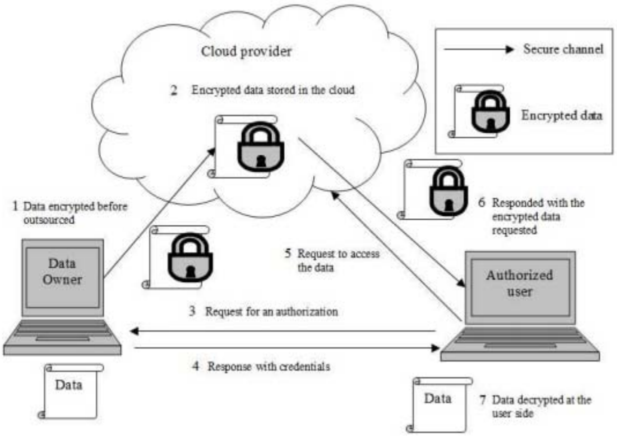
Cloud provider
2 Encrypted data stored in the cloud
Secure channel
Encrypted data
1 Data encrypted before outsourced
6 Responded with the encrypted data requested
5 Request to access the data
Data Owner
Authorized user
3 Request for an authorization
4 Response with credentials
Data
Data
7 Data decrypted at the user side

Fig 1.2- Cloud Computing Architecture for Preserving Data

The encrypting architecture of privacy before outsourcing the data on the cloud is shown in Figure 1.2. In the above architecture the data will stands in the encrypted shape & it can be decrypted by only the valid credential users. The decryption of data can be done only valid credentials cloud consumer's system. In the above design, the data privacy will remain independent for both the server trust as well as the SLA. Rather, the privacy protection of data only depends to the encryption algorithm techniques [7]. The other issues regarding that how the data owner and valid credential user's share as well as search their data that is encrypted. All these security measures should be done in a well defined manner so that the information should not get leaked to the intruders as well as the cloud providers [8]. The techniques of cryptography as well as the emerging data centric security approach may be the favorable solution to control the numerous challenges of cloud computing regarding the security.

4. SECURITY APPROACH TO CLOUD DATA SECURITY

In our approach, that we are going to discuss is Data Centric Security that stress the data security itself rather than the networks security etc. DCS is emerging speedily as the big enterprises are relying on digital information to run their big data and business. DCS allows overcome the organizations for the disconnection of Information technology securities and their business strategies. The DCS allows the mechanism to know about the stored data and also define the access policies of data on the cloud computing model [7].

The idea of DCS is based to furnish the security on cloud computing model at the data level. The owners of data are wholly responsible to define as well manage the security measures of data. These challenges can be accomplished without relying on the trusting the cloud computing provider [7]. Our proposed approach will use the various techniques for encryption and decryption. To overcome the management and computational expenses, the strategy of access control fulfillment and the symmetric key sharing of the data that are encrypted is accomplished by a well organized manner is based on the CRT. The enhancement of the security on the cloud paradigm to the data, the owner's should use a standard key itself to encrypt the data and then attach the unique key in a solid manner to the encrypted data. So that only the valid credential users can access the data with associated key. Moreover, the privacy can also be enhanced by keeping the authorized users identities hidden from the cloud computing provider [7]. Furthermore, secure search potential is the fundamental part on the encrypted data of our proposed solution as well as the necessary security standards, like the integrity etc. also attached to the data that are encrypted that will create the a secure file container, known as the DCS file [7]. This will allow only the valid user's for both to access as well as search the Data centric security file

When we look about the traditional techniques of protecting data, the security is provided to the server side that stores the data. To protect the data on clod the strategies are controlled by the server of the admin. Hence this way of approach is known as a system-centric approach that is not worthy to protect the consumer's important data on the untrusted cloud paradigm. Another approach known as the DCS is predicted to be worthy fruitful for the services of cloud. The data centric security shows in common that the protection focus of the security is throughout the data and that kind of terminology can be used differently. In the cloud paradigm, the primary approach of DCS is to protect the data from inside, which will provide the best security of data at any level life time where the actual data is stored [9].

As we know that the virtual storage devices are storing the data of consumer's in the cloud computing. The Models Software As A Service and Data As A Service, customers only own the stored data and the cloud service providers own all the software and hardware that are involved itself for processing and storing in data are totally owned by the service providers. In other public models such as the IaaS and PaaS models, the consumer's also own the software applications for handling their data. So, therefore, the most valuable asset of the customer is their data, that may contain their sensitive information.

The old security concept usually focuses about devices as well as the technologies used to hold and control the data. This traditional opinion is considered to be very harder by providing the accurate security for the secret as well as the sensitive data [10]. The research community of cloud focuses by securing the virtual machines as well as the operating systems that are hosting the services of cloud computing. There are various security standards based on the old security thought that focuses either virtual machine centric or system centric. All of the security thoughts are based on the concept of TC (Trusted Computing).

The focus of the trusted computing group is to develop the standards, so as to make the consumers data as well as the software applications in a way that will be fully hidden from the admin of the cloud. The technology standards based on the trusted computing group provides the tools that are used by the cloud consumers to monitor their data location on the cloud. The focus of Trusted Computing Group and Trust Platform Module tools are not by providing the cloud consumers with the desired security & privacy control for their data. Instead, the concept of TC allows the customers to monitor the operations [4]. Various researchers have suggested the DCS Approach for overcoming the security related issues of data on cloud by switch the focus of securing customer's data to the data itself. However, in the concept of DCS approach there are numerous ideas regarding that how it can be applied to the cloud computing paradigm.

In the DCS approach, security of data solutions for the cloud computing can be grouped on two standards:

- The first standard of classification is based on level by which the security is provided at.
- The second standard of classification is based on who is responsible for providing the security.

The security function levels that can be provided in relation of data are illustrated in Figure 1.3. In simple term, the focuses of explanation for providing the security from outside the data level are arranged as the SCS (system-centric security). And if the focus of solution is on a particular level, they will be classified as per their specific level. In Figure 1.2, the levels shown in the figure are average levels. However there can be extra or lesser levels based on the actual requirements and implementation in a practical system [7].

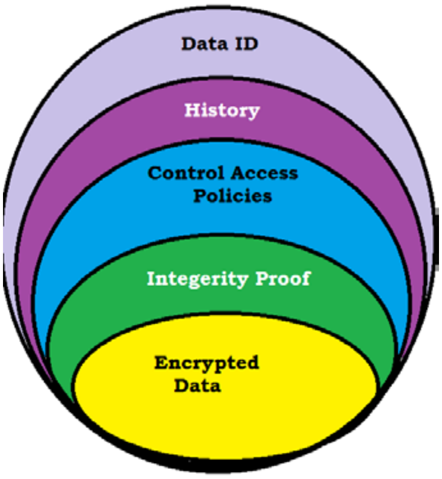

Fig: 1.3 – Data Centric Security

Another example of the second classification is illustrated below in Figure 1.4,

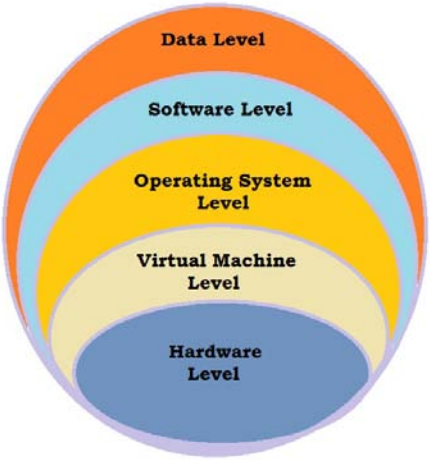

Fig: 1.4 –System Centric Security

In Figure 1.5, the security levels are three, namely service provider level, trusted computing level and the Data Centric Level [7].

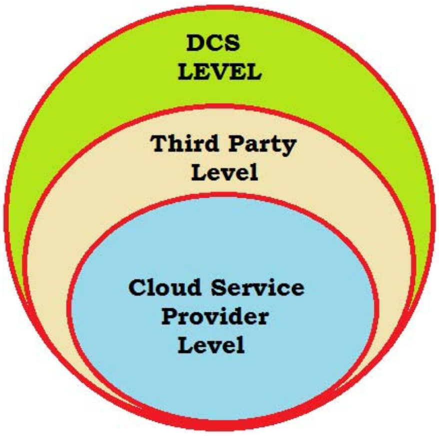

Fig: 1.5 – Cloud Computing Security Levels

The Securing issue of data is involved itself from the cloud computing system by the adoption of the Data centric concept. Various studies of the Data Centric Security is based on providing the security features from within the data However, the DCS depends on TC technologies for assessing the environment trustworthiness hence the data security requires an outside data security measure. The data centric view of securing and preserving privacy of data in the cloud is presented by providing data confidentiality and privacy access to the data using either the TC approach or the DCS approach where data are self-protected. Although, when the data have been transferred on the cloud computing paradigm the researchers are not agreed regarding that who is responsible, i.e., the owner of data, the third party or the provider, for the data security maintenance under the concept of data centric security.

5. CONCLUSION

The main important problem of cloud computing paradigm is the security of data. Various security standards are used to ensure the security of data on the cloud. In this paper we have proposed the DCS approach to enhance the security as well as the privacy of Consumers data that are stored in a cloud computing environment systems. Our paper proposes the framework to the cloud paradigm by applying the Data centric approach to improve the security as well as the privacy of data. In our proposed approach data is encrypted before it is outsourced to the cloud and creates a file known as DCS file that retrains the encrypted data and only the valid users can access the DCS file. Hence, the data remains secure against possible security risks from inside and outside the cloud environment even against possible malicious actions by the cloud provider itself.

6. ACKNOWLEDGEMENT

First and Foremost, Praises and Thanks To Almighty Allah. The satisfaction that accompanies that the successful completion of any task would be incomplete without the mention of people whose ceaseless cooperation made it possible, whose constant guidance and encouragement crown all efforts with success. I am grateful to my guide Dr. Pratima Gautam for the guidance, inspiration and constructive suggestions that helped me in the preparation of this progress report. I am extremely thankful to my parents and my Wife who have been always a source of inspiration for their never-ending support and love throughout the completion of this Paper and I am also thankful my friends who have helped in successful completion of the partial report.

7. REFERENCES:

[1] M. Malathi, "Cloud computing concepts," in Electronics Computer Technology (ICECT), 2011 3rd International Conference on,2011, pp. 236- 239.

[2] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," Computers &amp; Electrical Engineering, 2012

[3] N. el-Khameesy and H. A. Rahman, "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems," Journal of Emerging Trends in Computing and Information Sciences, vol. 3, 2012.

[4] S. Pearson, "Privacy, Security and Trust in Cloud Computing," Privacy and Security for Cloud Computing, 2012, pp. 3-42

[5] Yuraj Gupta, "Enhancing Data Security in Cloud Computing" International Journal of Scientific & Engineering Research, Vol 3, Issue 12, 2012

[6] Zaid Kartit. "Applying Encryption Algorithm To Enhance Data Security in Cloud Storage." Engineering Letters, Vol23, Issue 4, 2015.

[7] Nabil Giweli. "Enhancing Cloud Computing Security and Privacy". School of computing, engineering and mathematics, university of western sydney. 2013.

[8] W. Cong, W. Qian, R. Kui, and L. Wenjing, "Ensuring data storage security in Cloud Computing," in Quality of Service, 2009. IWQoS. 17th International Workshop on, 2009, pp. 1-9.

[9] Maninder Singh Bajwa , Hmani ; Sandeep Singh Kang "An Enhanced Data Owner Centric Model for Ensuring Data Security in Cloud "Advances in Computing and Communication Engineering (ICACCE), 2015 Second International Conference.

[10] Qin Liu, Guojun Wang ; Jie Wu ; Wei Chang "User-Controlled Security Mechanism in Data-Centric Clouds" High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conference on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference

AUTHOR PROFILE

JAHANGEER QADIREE[1] is pursuing his Doctors Degree in the discipline of Information Technology at Aisect University. He has received his Bachelors Degree in 2011 from Computer Application and Masters Degree in the discipline of Information Technology in the year 2014 from Aisect University.. His research area is Cloud Computing, Software Engineering, Data Mining, Social Networking,etc.