Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 48 (2015) 204 – 209

Procedia Computer Science

International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2015)

Conference Organized by Interscience Institute of Management and Technology,

Bhubaneswar, Odisha, India

Data Security Challenges and Its Solutions in Cloud Computing

R. Velumadhava Rao[a,*], K. Selvamani[b,*]

[a]*Department of Computer Science & Engineering, RIT, Chennai,india*
[b]*Department of Computer Science & Engineering, Anna University, Chennai, India*

Abstract

Cloud Computing trend is rapidly increasing that has an technology connection with Grid Computing, Utility Computing, Distributed Computing. Cloud service providers such as Amazon IBM, Google's Application, Microsoft Azure etc., provide the users in developing applications in cloud environment and to access them from anywhere. Cloud data are stored and accessed in a remote server with the help of services provided by cloud service providers. Providing security is a major concern as the data is transmitted to the remote server over a channel (internet). Before implementing Cloud Computing in an organization, security challenges needs to be addressed first. In this paper, we highlight data related security challenges in cloud based environment and solutions to overcome.

© 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of scientific committee of International Conference on Computer, Communication and Convergence (ICCC 2015)

*Keywords:*Cloud computing; Data secuity; Data Access

1. Introduction

Cloud Computing is the next generation internet based computing system which provides easy and customizable services to the users for accessing or to work with various cloud applications. Cloud Computing provides a way to store and access cloud data from anywhere by connecting the cloud application using internet [1]. By choosing the cloud services the users are able to store their local data in the remote data server [2]. The data stored in remote data

1877-0509 © 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of scientific committee of International Conference on Computer, Communication and Convergence (ICCC 2015)
doi:10.1016/j.procs.2015.04.171

center can be accessed or managed through the cloud services provided by the cloud service providers. So the data stored in a remote data center for data processing should be done with utmost care.

Cloud Computing security is the major concern to be addressed nowadays. If security measures are not provided properly for data operations and transmissions then data is at high risk [3]. Since cloud computing provides a facility for a group of users to access the stored data there is a possibility of having high data risk. Strongest security measures are to be implemented by identifying security challenge and solutions to handle these challenges. From Fig. 1 it is clear that how Data Security and Privacy are most important and critical factor to be considered.

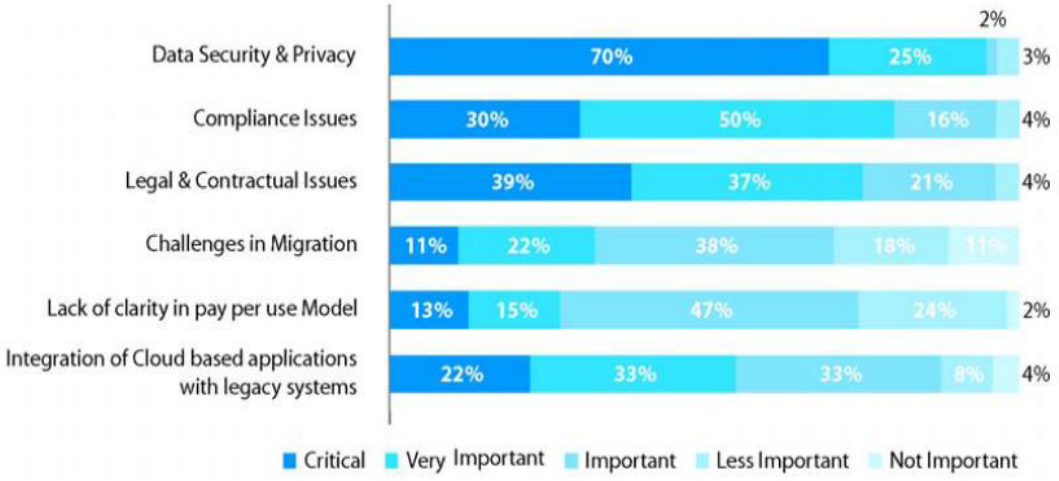

Fig. 1. Data Security and Privacy - Major Inhibitor to Cloud Adoption.

2. Literature Survey

Some of the proposed methods have been discussed in the literature survey for handling security issues in cloud computing.

Popovi and Hocenski, discussed about the security issues, requirements and challenges that are faced by cloud service providers during cloud engineering [4]. Behl explores the security issues related to the cloud environment. He also discussed about existing security approaches to secure the cloud infrastructure and applications and their drawbacks [5]. Sabahi discussed about the security issues, reliability and availability for cloud computing. He also proposed a feasible solution for few security issues [6]. Mohamed E.M et.al presented the data security model of cloud computing based on the study of cloud architecture. They also implemented software to enhance the work in Data Security model for cloud computing [7]. Wentao Liu introduced some cloud computing systems and analyzes cloud computing security problems and its strategy according to the cloud computing concepts [8]. Mathisen, E discussed about some of the key security issues that cloud computing are bound to be confronted with, as well as current implementations that provide a solutions to these vulnerabilities [9].

3. Models of Cloud Computing

Cloud Computing can be accessed via a set of cloud computing service models such as Software as a Service(SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In SaaS the services are provided by the service providers and customers make use of these services to run applications on a cloud infrastructure. These applications can be accessed through web browsers. PaaS is a way to rent hardware, operating systems, storage and network capacity over the internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones. In IaaS, the

consumer is provided with power to control process, manage storage, network and other fundamental computing resources which are helpful to manage arbitrary software.

4. Data Security Challenges

As we are moving into internet based cloud model, it requires great emphasis on Data Security and Privacy. Data loss or Data leakage can have severe impact on business, brand and trust of an organization. In Fig. 2. Data leak prevention is considered as most important factor with 88% of Critical and Very important challenges. Similarly Data Segregation and Protection has 92% impact on security challenges.

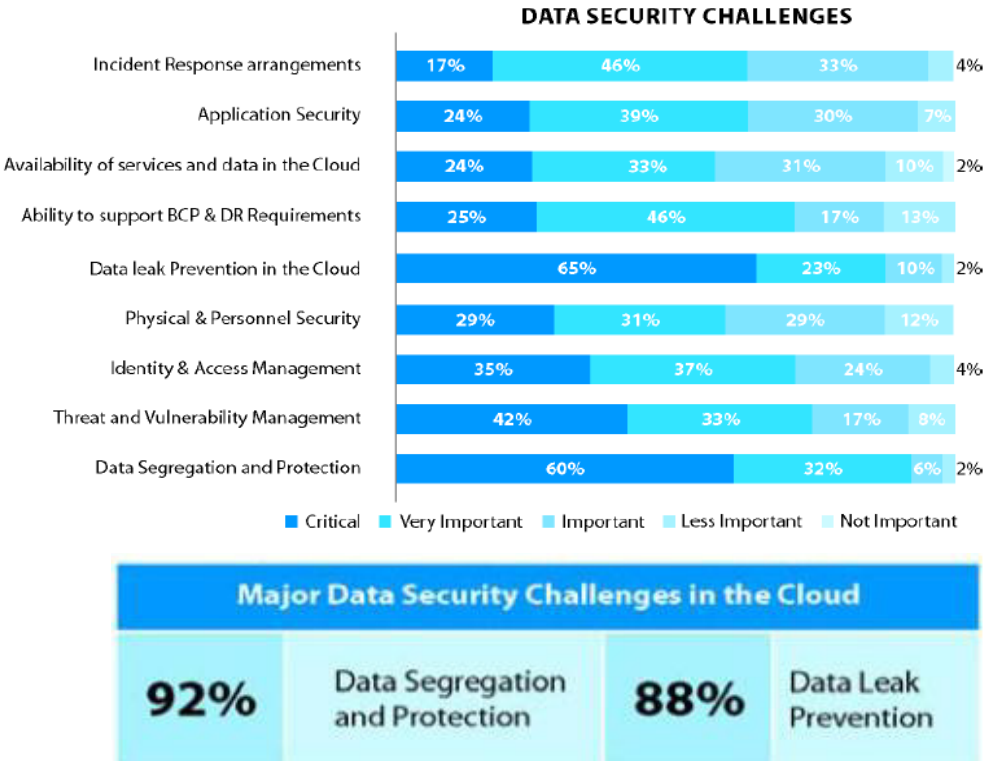

Fig. 2. Data Security Challenges.

4.1. Security

When multiple organizations share resources there is a risk of data misuse. So, to avoid risk it is necessary to secure data repositories and also the data that involves storage, transit or process. Protection of data is the most important challenges in cloud computing. To enhance the security in cloud computing, it is important to provide authentication, authorization and access control for data stored in cloud. The three main areas in data security are

Confidentiality: - Top vulnerabilities are to be checked to ensure that data is protected from any attacks. So security test has to be done to protect data from malicious user such as Cross-site Scripting, Access Control mechanisms etc..,.

Integrity: - To provide security to the client data, thin clients are used where only few resources are available. Users should not store their personal data such as passwords so that integrity can be assured.

Availability: - Availability is the most important issue in several organizations facing downtime as a major issue. It depends on the agreement between vendor and the client.

4.2. Locality

In cloud computing, the data is distributed over the number of regions and to find the location of data is difficult. When the data is moved to different geographic locations the laws governing on that data can also change. So there is an issue of compliance and data privacy laws in cloud computing. Customers should know their data location and it is to be intimated by the service provider.

4.3. Integrity

The system should maintain security such that data can be only modified by the authorized person. In cloud based environment, data integrity must be maintained correctly to avoid the data lost. In general every transactions in cloud computing should follow ACID Properties to preserver data integrity. Most of the web services face lot of problems with the transaction management frequently as it uses HTTP services. HTTP service does not support transaction or guarantee delivery. It can be handled by implementing transaction management in the API itself.

4.4. Access

Data access mainly refers to the data security policies. In an organization, the employees will be given access to the section of data based on their company security policies. The same data cannot be accessed by the other employee working in the same organization. Various encryption techniques and key management mechanisms are used to ensure that data are shared only with the valid users. The key is distributed only to the authorized parties using various key distribution mechanisms. To secure the data from the unauthorized users the data security policies must be strictly followed. Since access is given through the internet for all cloud users, it is necessary to provide privileged user access. User can use data encryption and protection mechanisms to avoid security risk.

4.5. Confidentiality

Data is stored on remote servers by the cloud users and content such as data, videos etc.., can be stored with the single or multi cloud providers. When data is stored in the remote server, data confidentiality is one of the important requirements. To maintain confidentiality data understanding and its classification, users should be aware of which data is stored in cloud and its accessibility.

4.6. Breaches

Data Breaches is another important security issue to be concentrated in cloud. Since large data from various users are stored in the cloud, there is a possibility of malicious user entering the cloud such that the entire cloud environment is prone to a high value attack. A breach can occur due to various accidental transmission issues or due to insider attack.

4.7. Segregation

One the major characteristics of cloud computing is multi-tenancy. Since multi-tenancy allows to store data by multiple users on cloud servers there is a possibility of data intrusion. By injecting a client code or by using any application, data can be intruded. So there is a necessity to store data separately from the remaining customer's data. Vulnerabilities with data segregation can be detected or found out using the tests such as SQL injection aws, Data validation and insecure storage.

4.8. Storage

The data stored in virtual machines have many issues one such issue is reliability of data storage. Virtual machines needs to be stored in a physical infrastructure which may cause security risk.

4.9. Data Center Operation

In case of data transfer bottlenecks and disaster, organizations using cloud computing applications needs to protect the user's data without any loss. If data is not managed properly, then there is an issue of data storage and data access. In case of disaster, the cloud providers are responsible for the loss of data.

5. Solutions to Data Security Challenges

Encryption is suggested as a better solution to secure information. Before storing data in cloud server it is better to encrypt data. Data Owner can give permission to particular group member such that data can be easily accessed by them. Heterogeneous data centric security is to be used to provide data access control. A data security model comprises of authentication, data encryption and data integrity, data recovery, user protection has to be designed to improve the data security over cloud. To ensure privacy and data security data protection can be used as a service.

To avoid access of data from other users, applying encryption on data that makes data totally unusable and normal encryption can complicate availability. Before uploading data into the cloud the users are suggested to verify whether the data is stored on backup drives and the keywords in files remain unchanged. Calculate the hash of the file before uploading to cloud servers will ensure that the data is not altered. This hash calculation can be used for data integrity but it is very difficult to maintain it. RSA based data integrity check can be provided by combining identity based cryptography and RSA Signature. SaaS ensures that there must be clear boundaries both at the physical level and application level to segregate data from different users. Distributed access control architecture can be used for access management in cloud computing. To identify unauthorized users, using of credential or attributed based policies are better. Permission as a service can be used to tell the user that which part of data can be accessed. Fine grained access control mechanism enables the owner to delegate most of computation intensive tasks to cloud servers without disclosing the data contents. A data driven framework can be designed for secure data processing and sharing between cloud users. Network based intrusion prevention system is used to detect threats in real-time. To compute large files with different sizes and to address remote data security RSA based storage security method can be used.

6. Conclusions and Future Work

Although cloud computing is the new emerging technology that presents a good number of benefits to the users, it faces lot of security challenges. In this paper data security challenges and solutions are provided for these challenges to overcome the risk involved in cloud computing. In future concrete standards for cloud computing security can be developed. To provide a secure data access in cloud, advanced encryption techniques can be used for storing and retrieving data from cloud. Also proper key management techniques can be used to distribute the key to the cloud users such that only authorized persons can access the data.

References

1. L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner. A break in the clouds: towards a cloud definition, in: ACM SIGCOMM Computer Communication Review, 2008.p.50-55.
2. M.B. Mollah, K.R. Islam, and S.S. Islam. Next generation of computing through cloud computing technology, in: 2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), May 2012.p.1-6.
3. Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable and fine-grained data access control in cloud computing, in: IN-FOCOM, 2010 Proceedings IEEE, 2010.p.1-9.

4. Kresimir Popovic and Zeljko Hocenski. Cloud computing security issues and challenges, in: MIPRO, 2010 Proceedings of the 33rd International Convention, 2010.p.344-349.
5. Akhil Bhel, Emerging Security Challenges in Cloud Computing. Information and Communication Technologies, in: 2011 World Congress on, Mumbai, 2011.p.217-222.
6. Farzad Sabahi. Cloud Computing Security Threats and Responses, in: IEEE 3rd International Conference on Communication software and Networks(ICCSN), May 2011.p.245-249.
7. Eman M.Mohamed, Hatem S Abdelkader, Sherif EI Etriby. Enhanced Data Security Model for Cloud Computing, in:8th International Conference on Informatics and Systems(INFOS), Cairo, May 2012.p.12-17.
8. Wentao Liu. Research on Cloud Computing Security Problem and Strategy, in: 2nd International Conference on Consumer Electronics. Communications and Networks (CECNet), April 2012.p.1216-1219.
9. Eystein Mathisen. Security Challenges and Solutions in Cloud Computing, in: International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), 2011.p.208-212.