International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 3, ISSN No. 2455-2143, Pages 225-227
Published Online July 2020 in IJEAST (http://www.ijeast.com)

HOW CLOUD COMPUTING WORK AND PROTECT THE DATA OF END USER

Akash Pandey
BCA Student
Computer Science Department,
Kalinga University, Atal Nagar,
Chhattisgarh, India

Rahul Kumar Chawda
Assistance professor
Computer Science Department,
Kalinga University, Atal Nagar,
Chhattisgarh, India

ABSTRACT - Cloud computing may be a good platform for research and application of knowledge mining, for the rationale that it provides powerful capacities of storage and computing, excellent resource management based on virtualization and resource sharing model, and comprehensive service system.

However, investigation on data processing in cloud computing environment remains in its infancy.

In this paper, solvent of classification rules mining with resources in cloud is developed, and an innovative classification rules mining model with genetic algorithm in cloud computing is proposed considering characteristics of cloud computing. An illustrative example is analyzed to show feasibility and effectiveness of the suggested model.

I. INTRODUCTION

This chapter assumes that the reader is familiar with the manner in which cloud computing is defined as set forth by the National Institute of Standards and Technology, a federal agency of the United States Government.

In brief, cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing. This cloud model is composed of five essential characteristics, three service models, and four deployment models

II. CLOUD COMPUTING AND IDENTITY

- This is a bold statement, but nonetheless appears to be the method of choice by a number of industry leaders.

- However, as well as being a perceived panacea for the ills of data security, it is also one of the most difficult technological methods to get right. Identity, of all the components of information technology, is perhaps the most closest to the heart of the individual.

- After all, our identity is our most personal possession and a digital identity represents who we are and how we interact with others online. The current state of the art in digital identity, in particular with reference to cloud identities, is a work in progress, which by the time you are reading this should hopefully be entering more maturity.

- However, going back to my opening statement, digital identity can be used to form the basis of data security, not only in the cloud but also at the local network level too. To expand on this somewhat, we need to look at the link between access, identity, and risk. These three variables can become inherently connected when applied to the security of data, because access and risk are directly proportional:

- As access increases, so then risk to the security of the data increases. Access controlled by identifying the actor attempting the access is the most logical manner of performing this operation. Ultimately, digital identity holds the key to securing data, if that digital identity can be programmatically linked to security policies controlling the post access usage of data.

- The developments seen in the area of a cloud-based digital identity layer have been focused on creating a ―user-centric‖ identity mechanism. User- centric identity, as opposed to enterprise-centric identity, is a laudable design goal for something that is ultimately owned by the user. However, the Internet tenet of ―I am who I say I am‖ cannot support the security requirements of a data protection

methodology based on digital identity, therefore digital identity.

III. OVERVIEW OF LEGAL ISSUES

- The legal issues that arise in cloud computing are wide ranging. Significant issues regarding privacy of data and data security exist, specifically as they relate to protecting personally identifiable information of individuals, but also as they relate to protection of sensitive and potentially confidential business information either directly accessible through or gleaned from the cloud systems (e.g., identification of a company‘s customer by evaluating traffic across the network).

- Additionally, there are multiple contracting models under which cloud services may be offered to customers (e.g., licensing, service agreements, on-line agreements, etc.).

- The appropriate model depends on the nature of the services as well as the potential sensitivity of the systems being implemented or data being released into the cloud. In this regard, the risk profile (i.e., which party bears the risk of harm in certain foreseeable and other not-so-foreseeable situations) of the agreement and the cloud provider‘s limits on its liability also require a careful look when reviewing contracting models.

- Additionally, complex jurisdictional issues may arise due to the potential for data to reside in disparate or multiple geographies. This geographical diversity is inherent in cloud service offerings. This means that both virtualization of and physical locations of servers storing and processing data may potentially impact what country‘s law might govern in the event of a data breach or intrusion into cloud systems.

IV. THE CURRENT STATE OF DATA SECURITY IN THE CLOUD

- However, the very nature of cloud computing dictates that data are fluid objects, accessible from a multitude of nodes and geographic locations and, as such, must have a data security methodology that takes this into account while ensuring that this fluidity is not compromised. This apparent dichotomy data security with open movement of data—is not as juxtaposed as it first seems. Going back to my previous statement that security is better described as ―risk mitigation, ‖ we can then begin to look at securing data as a continuum of choice in terms of levels of accessibility and content restrictions: This continuum allows us to choose to apply the right level of protection, ensuring that the flexibility bestowed by cloud computing onto the whole area of data communication is retained.

- As I write, the IT industry is beginning to wake up to the idea of content- centric or information-centric protection, being an inherent part of a data object. This new view of data security has not developed out of cloud computing, but instead is a development out of the idea of the ―deperimerization‖ of the enterprise. This idea was put forward by a group of Chief Information Officers (CIOs) who formed an organization called the Jericho Forum.

- The Jericho Forum was founded in 2004 because of the his type of data exchange in a secure manner. However, the ideas forwarded by the Jericho Forum are also applicable to cloud computing. The idea of creating, essentially, de-centralized perimeters, where the perimeters are created by the data object itself, allows the security to move with the data, as opposed to retaining the data within a secured and static wall. This simple but revolutionary change in mindset of how to secure data is the ground stone of securing information within a cloud and will be the basis of this discussion on securing data in the cloud.

V. CONCLUSION

Hrere, all concept of the topic that is Cloud Computing cover the all the issue of the storage and and security of the data. Basically Cloud computing is recently new technology that has potiantial to have a great impact of the computer science world.

VI. REFERENCE

1 http://www.infoworld.com/article/08/04/07/15FE-cloud-computing-reality_1.html,. (2008). “What Cloud Computing Really Means”. Retrieved from . http://www.infoworld.com/article/08/04/07/15FE-cloud-computing-reality_1.html,

2 Peter Mell and Timothy Grace, “ The NIST Definition of Cloud Computing (Draft)”, Recommendations of the National Institute

of Standards and Technology, 7 pages (January.2011).

3 M.Tariq Banday, Jameel A. Qadri and Nisar A. Shah, " Study of Botnets and Their Threats to Internet Security", Sprouts – Working Papers on Information Systems.

4 Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose and Andreas Terzis, " A Multifaceted Approach to Understanding the Botnet Phenomenon".

5 http://en.wikipedia.org/wiki/Cloud_computing

6 Degado R., https://datafloq.com/read/opportunitieschallenges-cloud-computing-big-data/4456

7 Robinson S., (2012, 2015), ―The Storage and Transfer Challenges of Big Data.Accessed‖,

8 http://sloanreview.mit.edu/article/the-storage-andtransfer-challenges-of-big-data/.

9 Chen J., Chen Y., Du X., Li C., Lu J., Zhao S., and Zhou X.., (2013), ―Big Data Challenge: A Data Management Perspective.‖ Frontiers of Computer Science 7 (2) (Pg157–164).