Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 65 (2015) 853 – 858

Procedia Computer Science

International Conference on Communication, Management and Information Technology (ICCMIT 2015)

Security Issues Over Some Cloud Models

Passent M. El-Kafrawy[a], Azza A. Abdo[a], Amr. F. Shawish

Faculty of Science, Menoufia University, Menofia, Egypt
basant.elkafrawi@science.menofia.edu.eg

Abstract

Cloud computing is an uprising field in information technology (IT) industry because of its performance, high availability, low cost and much more. The data leakage, lack of proper security control policy, and weakness in the data sentry are the main worries of the companies. So that a cloud data security models should be able to overcome all the possible issues of cloud computing, so as to provide the benefits of cloud computing and preventing the owner's data from all the risks associated. This paper focuses on two phases; the first phase is a discussion of the security functions that should be realized during building any data cloud model. A comparison of some designed cloud models is discussed as the second phase. The cloud models discussed are Wang scheme (2009), Prased scheme (2011), Sandeep K. Sood (2012), Xin Dong scheme (2014), and P. Lavanya scheme (2014) all of which are displayed and its security are discussed. A discussion of a number of possible security measures is our concern in this paper, which should be considered in any cloud based model. Recommendations are further given for proper security issues over cloud systems.

Peer-review under responsibility of Universal Society for Applied Research

Keywords: Cloud computing, Security factors

1. Introduction

As a matter of fact IT is a set of tools, methodologies, and tasks with the required equipment to collect, process, and provide information. Generally, speaking, IT is used for office automation, multimedia, and telecommunication. IT challenges are, Globalization, Aging Data Centers, Storage Growth, Application Explosion, Cost of ownership and

Peer-review under responsibility of Universal Society for Applied Research
doi:10.1016/j.procs.2015.09.041

Acquisitions. The IT challenges have made organizations think about the Cloud Computing model to provide better service to their customers. Cloud computing is internet-based computing in which large groups of remote servers are networked to allow the centralized data storage, and online access to computer services or resources. Cloud computing generally has five characteristics: rapid elasticity, measured service and on-demand self-service: resources can be provisioned via automated mechanisms [1]. There are four common deployment models for cloud services loosely determined by who has access to the cloud services: Public Cloud, Private Cloud, Community Cloud, and Hybrid Cloud [2]**. Cloud computing security** or, more simply cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing [3].

The data leakage, lack of proper security control policy, and weakness in the data sentry are fears of the companies. So that cloud data security models should be able to overcome all the possible issues of cloud computing, so as to provide the benefits of cloud computing and preventing the owner's data from all the risks associated.

Moving applications to the cloud and accessing the benefits means first evaluating specific data security issues and cloud security issues**.** When companies move applications from on-premise to cloud-based, challenges arise from data residency, industry compliance requirements, privacy and third party obligations concerning the treatment of sensitive data. Corporate policies or the regulations of the governing jurisdictions impact the way sensitive data is managed including where it is located, what types of data can be collected and stored and who has access to it. These issues can determine the degree to which organizations can realize the value of cloud computing. Cloud security issues fall primarily into three areas: **1- Data Residency** - Many companies face legislation by their country of origin or the local country that the business entity is operating in, requiring certain types of data to be kept within defined geographic borders. There are specific regulations that must be followed, centered around data access, management and control. **2- Data Privacy** - Business data often needs to be guarded and protected more stringently than non-sensitive data. The enterprise is responsible for any breaches to data and must be able to ensure strict cloud security in order to protect sensitive information. **3- Industry & Regulation Compliance** - Organizations often have access to and are responsible for data that is highly regulated and restricted. Many industry-specific regulations such as GLBS, CJIS, ITAR and PCI DSS, require an enterprise to follow defined standards to safeguard private and business data and to comply with applicable laws. Cloud computing security issues include preserving confidentiality and privacy of data, authorization, authentication and integrity. We shall investigate some security functions to solve security issues on the cloud.

This paper focuses on two phases; the first phase is a discussion of the security functions that should be realized during building any data cloud model to cover security issues. A comparison of some designed cloud models are discussed as the second phase. In this paper, the five algorithms Wang's scheme (2009) [7], Prased's scheme (2011) [9], Sandeep K. Sood (2012) [10], P. Lavanya's scheme (2014) [11] and Xin Dong's scheme (2014) [12] are described. Also we analyze these five algorithms focusing on the security factors defined in section 2. In addition to these factors, we put additional factors such as scalable data sharing, privacy, fake identity and balance security and usability, which will be defined in section 4 as requirements for secure cloud systems.

This paper is designed as following, Section 2 illustrates the security functions over cloud computing. Section 3 related work on the cloud models. Comparison of algorithms is presented in Section 4. Finally conclusion is given in in section 5.

2. Security functions over cloud computing

An efficient cloud data security model should be able to overcome all the possible issues of cloud computing, so as to provide the benefits of cloud computing to reach its maximum heights and propel in the direction it is designed for, by preventing the owner's data from all the risks associated and gives for cloud model more security and efficiency. The security functions over cloud computing are listed as following: