Hybrid Data Security Model for Cloud

Sandeep K. Sood, Department of Computer Science & Engineering, Guru Nanak Dev University Regional Campus, Gurdaspur, Punjab, India

ABSTRACT

Security of data is one of the main concern in the implementation of cloud computing. This paper proposes a highly effective and efficient cloud security model. The proposed security model keeps the most critical data on the private cloud and the rest of it on the public cloud. It uses hash codes to check the integrity of the data at the public cloud. The proposed cloud security model provides the provision of defining user roles thereby determining the type of access the user exercises on the data. This model uses dual verification mechanism for user authentication by using username and password on one layer and key authentication on another layer. A cryptographic process is used to make the overall security of the data on the cloud highly robust. A comprehensive security analysis of the model is done against various types of attacks and the results are very promising. This model is compared to various existing cloud security models and the results shows that our technique is faster, much more robust and efficient as compared to other existing models. This model is cost effective because it uses private cloud only for highly sensitive data. Rest of data is stored on the public cloud, where data storage cost is comparatively very less.

Keywords: Cloud Computing, Cryptographic Process, Dual Verification, Hash Codes, Private Cloud, Public Cloud

1. INTRODUCTION

Cloud computing is predicted to be the next big revolution in the computing industry. It is a dynamically scalable, network based computing environment where the resources required by the user are allocated as per requirement and revoked when the user completes the task. It follows a utility based model in which the user pays as per resource utilization at the cloud. This characteristic of cloud computing makes it cheaper than the existing computing environments and always availability of computational resources to the end user. The cloud can cater to end user with its faster computation and highly scalable pool of resources (Sood, 2013). These resources can be in the form of memory, processing time, processing power, application software, software development platforms, storage space etc (Overby, Bharadwaj, & Sambamurthy, 2006). It effectively addresses the computing needs of users ranging from an individual to large organizations. One aspect of the cloud which obstructs the users from using cloud services is data security. Data security in cloud is a highly complex issue. The data

DOI: 10.4018/ijcac.2013070104
owner’s especially large organizations fear that their data can be misused by the cloud provider without their knowledge. This concern is a major hurdle in the path of shifting operations to the cloud. An effective security model addressing all these concerns is proposed in this paper.

This paper proposes a hybrid cloud computing model which effectively handles the issues related to cloud data security including confidentiality, integrity, authentication and authorization. The model handles both external as well as internal data security threats. It makes use of a hybrid cloud architecture using both private as well as public cloud (Daniel & Wilson, 2003). A dual security layer is used in proposed model. One is authentication based on username and password and the other is that the user should possess the key to decrypt a password stored at the cloud, without which the password filled by the user and the password stored on cloud cannot be compared. This completes the user authentication phase of the proposed security model. For user authorization, a user role is associated with each user and stored in the database of cloud. The user can only perform operations with respect to this role. This role is determined by the data owner. Also, for processing data at the cloud and keeping it safe even from the cloud service provider, a cryptographic process is proposed. If the user is authenticated and authorized then the operations requested on the data are performed including manipulation and processing of the data. This is done by invocation of a cryptographic process which takes a key defined by the data owner in executable form as input from cloud database and loads into memory. This process decrypts the data, caters it to requesting processes and encrypts it before storing it back (Dikaiakos, Katsaros, Pallis, Vakali, & Mehra, 2009). Symmetric key encryption is used for both decrypting and encrypting data. Since the key is in executable form so it is safe from any modifications by the cloud service provider. Also the cryptographic process is made a part of the operating system therefore, eliminating the control of cloud on this process (Little, 2003).

The paper is organized as follows. In Section 2, related work to security of data in cloud is presented. In Section 3, a data security model for cloud is proposed. In Section 4, security analysis of the proposed model is performed against various data security attacks. Section 5 compare the cost and functionality analysis of the proposed model with other existing related models and Section 6 concludes the paper.

2. RELATED WORK

There are number of models and techniques proposed for increasing data security and access control at the cloud. These works use encryption for securing data at the cloud, analyze the various risks involved with keeping data at the cloud and propose the establishment of trusted third party services at the cloud. In 2010, Farrell (2010) discussed the various kinds of risks associated with cloud computing. These risks are evaluated with respect to various cloud computing models such as Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). This paper does not discuss anything regarding the solution to these problems and hence only creates awareness about the various security issues associated with the cloud. Our proposed model solves most of the issues that are mentioned in Farrell’s (2010) work. Also in 2010, Julisch and Hall (2010) proposed the use of virtual information security management system, which can help to improve information security, but the proposed technique is complex as compared to the one proposed in our model. Our proposed model helps to reach an optimal security level without compromising on performance and is better than most existing models. The results are promising and the level of security is high compared to other existing models thereby enhancing data security at the cloud on all fronts.

In 2011, Zhou et al. (2011) proposed a cloud computing technique using role based encryption to secure data at the cloud. In this technique, the data at the cloud is encrypted
Personality Traits and Consumer Behavior in the Mobile Context: A Critical Review and Research Agenda
www.igi-global.com/article/personality-traits-consumer-behavior-mobile/59964?camid=4v1a