An Approach to Data Confidentiality Protection in Cloud Environments

Stephen S. Yau, Information Assurance Center and School of Computing, Informatics and Decision Systems Engineering, Arizona State University, Tempe, AZ, USA

Ho G. An, Information Assurance Center and School of Computing, Informatics and Decision Systems Engineering, Arizona State University, Tempe, AZ, USA

Arun Balaji Buduru, Information Assurance Center and School of Computing, Informatics and Decision Systems Engineering, Arizona State University, Tempe, AZ, USA

ABSTRACT

In current cloud computing systems, because users' data is stored and processed by computing systems managed and operated by various service providers, users are concerned with the risks of unauthorized usage of their sensitive data by various entities, including service providers. The current cloud computing systems protect users' data confidentiality from all entities, except service providers. In this paper, an approach is presented for improving the protection of users' data confidentiality in cloud computing systems from all entities, including service providers. The authors' approach has the following features: (1) separation of cloud application providers, data processing service providers and data storage providers, (2) anonymization of users' identities, (3) grouping cloud application components and distributing their execution to distinct cloud infrastructures of data processing service providers, and (4) use of data obfuscation and cryptography for protecting the sensitive data from unauthorized access by all entities, including service providers. The proposed approach ensures that users' sensitive data can be protected from their service providers even if the users do not have full cooperation from their service providers.

Keywords: *Anonymization of User Identities, Cloud Environments, Data Confidentiality, Data Obfuscation, Service Providers*

INTRODUCTION

Due to its many benefits, including cost effectiveness, high scalability and flexibility, cloud computing has gained significant momentum as a major paradigm for outsourcing computing for various applications, especially for business applications. However, because users' data in cloud environments is processed and stored on remote machines owned and operated by various service providers, not under the control of users, one of the most important limitations on broadening adoption of cloud computing by various critical applications is due to the

DOI: 10.4018/jwsr.2012070104

serious concerns on its capability of protecting the confidentiality of users' sensitive data from various entities ranging from those developing, managing, serving to those using cloud computing (Rocha, Abreu, & Correia, 2011). Since current access control mechanisms in cloud computing systems used to protect the confidentiality of users' data from unauthorized entities do not include the service providers of cloud computing systems (Yu, Wang, Ren, & Lou, 2010), and since users' data can be processed only in unencrypted form, service providers may have unauthorized access and use their users' confidential data. Hence, an effective approach to protecting users' data confidentiality from all entities, including the service providers, is needed.

Current cloud computing systems have the following properties and consequences for protecting users' data confidentiality from the service providers of cloud computing systems:

- Each service provider has its own software layer, platform layer and infrastructure layer. When a user has a cloud application, the user is forced to use the software, platform and infrastructure provided by the same service provider, and hence the service provider has access privileges to the users' data.
- The user is forced to use the interfaces provided by the service providers, and users' data has to be in a fixed format specified by the service providers, and hence the service providers can understand users' data.

It is obvious that if the service providers do not have the access privileges to the users' data and/or cannot understand users' data, then the service providers will not be able to use users' data without users' authorization. In this paper, we will present an approach to develop cloud applications in such a way that will prevent data processing service providers and data storage providers from accessing and understanding users' confidential data in cloud computing systems. In our approach, cloud application providers, data storage providers and data processing service providers are separated into three distinct entities. In our approach, combination of data obfuscation, cryptography, anonymization of users' identities and grouping of the components of each cloud application are used to protect confidentiality of users' sensitive data. It is noted that since there are many existing cryptographic techniques (Stallings, 2010); appropriate cryptographic techniques based on the protection requirements of the transmitted data can be selected and used in our approach.

This paper is organized as follows. We will first discuss the current state of art related to our approach and present our overall approach. In the subsequent sections, we will first discuss how to anonymize users' identities for protecting users' data confidentiality in cloud computing systems and then discuss how cloud application providers can develop and group the components of a cloud application such that the application software can be executed in distinct infrastructures of data processing service providers without disclosing confidentiality of users' sensitive data. Then, we will discuss how to use data obfuscation during the execution of application components in cloud computing.

RELATED WORK

In this section, we will discuss the current state of art related to our approach. An approach was developed for users to manage the privacy of their data in clouds through data obfuscation, privacy policy settings, auditing and monitoring of personal data in clouds (Mowbray & Pearson, 2009). In this approach, a user-centric trust model was presented to help users control their sensitive information in clouds. However, this approach uses data obfuscation from the data processing service providers and hence there is no protection of users' data confidentiality against the data processing service providers during data processing.

To protect the identities of the users who want to maintain their anonymity in clouds, an approach was developed to adapt clouds to protect users' real identities and their data

Using Markov Decision Process Model with Logic Scoring of Preference Model to Optimize HTN Web Services Composition

Jiuyun Xu, Kun Chen and Stephan Reiff-Marganiec (2011). *International Journal of Web Services Research (pp. 53-73).*

www.igi-global.com/article/using-markov-decision-process-model/55236?camid=4v1a