King Saud University

Journal of King Saud University – Engineering Sciences

SHORT COMMUNICATION

A secure data privacy preservation for on-demand cloud service

CrossMark

Chandramohan Dhasarathan *, **Vengattaraman Thirumal,**
Dhavachelvan Ponnurangam

Department of Computer Science, School of Engineering & Technology, Pondicherry University, Pondicherry, India

Abstract   This paper spotlights privacy and its obfuscation issues of intellectual, confidential information owned by insurance and finance sectors. Privacy risk in business era if authoritarians misuse secret information. Software interruptions in steeling digital data in the name of third party services. Liability in digital secrecy for the business continuity isolation, mishandling causing privacy breaching the vicinity and its preventive phenomenon is scrupulous in the cloud, where a huge amount of data is stored and maintained enormously. In this developing IT-world toward cloud, users privacy protection is becoming a big question , albeit cloud computing made changes in the computing field by increasing its effectiveness, efficiency and optimization of the service environment etc, cloud users data and their identity, reliability, maintainability and privacy may vary for different CPs (cloud providers). CP ensures that the user's proprietary information is maintained more secretly with current technologies. More remarkable occurrence is even the cloud provider does not have suggestions regarding the information and the digital data stored and maintained globally anywhere in the cloud. The proposed system is one of the obligatory research issues in cloud computing. We came forward by proposing the Privacy Preserving Model to Prevent Digital Data Loss in the Cloud (PPM–DDLC). This proposal helps the CR (cloud requester/users) to trust their proprietary information and data stored in the cloud.
© 2015 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

* Corresponding author.
  E-mail addresses: pdchandramohan@gmail.com (D. Chandramohan), vengattaraman.t@gmail.com (T. Vengattaraman), dhavachelvan@gmail.com (P. Dhavachelvan).
Peer review under responsibility of King Saud University.

ELSEVIER | **Production and hosting by Elsevier**

1. Introduction

Cloud computing is one of the massive and major research areas in both the industrial and academic fields and many researchers have been working toward its research issues. As the cloud came into existence a lot of issues also surrounded it. Normally cloud computing has mostly common and general issues like interoperability, SLA-(service level agreement), universal standards, unique approach for all cloud providers, data

portability among different clouds, various security issues and mainly privacy protection to users secret and confidential information. The cloud elucidation is interoperable and companionship with homogeneous services to benefits all sorts of business needs at earliest without effecting the privacy. CP consists of different layers for information dealing and on-demand provisioning of computational resources.

Data stored in the cloud are accessible to users in the form of different services with the help of traditional networks and it is also known to be the cloud storage, in which it holds a brief description about cloud user profiles, business details and back up information to make available ubiquitously via internet as backbone. Online data backup, data archiving, data compliances, disaster recovery, and compliance regulations are some of the issues in cloud data storage. Many technologies have been developed for cloud data storage and portability of information transfer among different cloud providers and it is mainly based on the cloud provider's service level agreements and policy. In this fast developing cloud business world users are permitted to exchange their data stored from one provider to other as a portability option.

In this context the providers should ensure the privacy protection strategies or enrich the issues pertained along with their storage and recovery. Leading cloud providing companies are farm-outing their customers information to cloud back up service providers as an infrastructure and power maintenance policy. To reduce the doubt or increase trust among user's about their information management, some nominal metrics should be adopted to identify the maximum possibility of storing information. There may be many risk factors evaluated along with this as a data offsite replication and data disaster recovery as a privacy issue for both providers and consumers. At administration level the need for cloud storage as been adopted in several principles to serve their clients on demand at all circumstances with high privacy and security.

2. Background and related work

To avoid unlawful information disclosures Breaux and Anton, 2008, derived a method to support the software engineering effort to derive security requirements from regulations; in which the methodology for directly extracting access rights and obligations from regulation texts. The methodology provides statement-level coverage for an entire regulatory document to consistently identify and infer six types of data access constraints and assign required priorities between access rights and obligations. Liu and Chen (2011), designed a VGuard framework with an efficient protocol that allows a cloud policy owner and a cloud request owner to collaboratively determine whether the request satisfies the policy without the policy owner knowing the request and the request owner knowing the policy. Xiong et al. (2011), proposes a cost-aware resource management system based on SLA-service level agreement termed as SmartSLA which consists of two main components: the system modeling module and the resource allocation decision module. To prevent the online social community Li et al. (2011), shows his interest in group based privacy-preserving recommender system called Pistis. The identification of inherent item-user's interest group and separating them with private interests and public interest might improve the solidity, and help to fasten and accurately

transmit emergency data Liang et al. (2011), through an emergency call scheme by enabling patients in life-threatening emergencies to call the nearby helpers via mobile healthcare social networks. To facilitate interoperations among the applied cryptographic mechanisms Lee et al. (2011), applied the policy regulation with the HIPAA (Health Insurance Portability and Accountability Act), for a flexible cryptographic key management solution. Chandramohan et al. (2014, 2015a,b), proposed a testbed for evaluating the efficiency of services by filtering its functional and non functional QOS-(Quality of Services) parameters. Web service personalization and suitability in cloud as mathematical evaluation the QOS parameters are verified for different service efficiency.

Kadloor et al. (2012), proposal to develop a dynamic program to compute the optimal privacy preserving policy that minimizes the correlation between user's traffic and adversary's waiting times of the cloud user. Hong et al. (2012), propose a new MapCG model as a map-reducing framework to provide source code level portability between CPUs (central processing units) and GPUs (graphics processing units). Chang and Choi (2010), cloud computing is the upcoming trend in the IT business world and faces a lot of challenges in technical matters and security issues. In his proposal the author described the crucial needs of cloud computing technological features, and challenges and also cloud computing security. Hussin et al. (2012), proposed a new era of using privacy manager in the cloud to control all features of cloud providers and to control all their policy based obfuscation and de-obfuscation. To enhance the usability of this approach the author proposed his own approach to evaluate the performance and its scalability. Chandramohan et al. (2012), provided a protocol for authentication purpose with an user identity based key management system to minimize the data lose.

Pieters (2011), describes the major research issues in recent development in the cloud and its security issues, the ethical implication and privacy issues can be viewed and monitored using his proposed bird's eye view approach. In his approach he covered the disappearing boundary of the cloud and encryption standards in use, its physical security properties etc. Ruiter and Warnier (2011), in his approach describes the privacy regulations for cloud leads to the occurrence of uncertainty. Troncoso-Pastoriza and Perez-Gonzalez (2010), expresses the landscape signal processing cryptographic technique to maintain the private information of cloud users and clients of cloud providers. The author briefly explains the fundamental background of the cloud and its issues from the day it originates. Vaquero et al. (2011), describes many issues and problems getting increased daily in the cloud and the author proposed a few access controls and encryption techniques to solve the privacy issues in cloud computing virtualized data centers. Grodzinsky and Tavani (2011), adopts the Helen Nissenbaum's theory as a framework of privacy as contextual integrity for evaluating the cloud providers services, which depends on decision heuristic model. Murugaiyan et al. (2014), describes the preventing mechanism for cloud user and their data could be organized using a framework approach. While addressing the cloud concepts over the past several years there presents many cloud computing service models and the risk migration in it. The main goal to standardize the service level agreements and policies adapted for maintaining privacy and enhancing the security in cloud describes