Eleyon
SOUTH ASIAN JOURNAL OF ENGINEERING AND TECHNOLOGY

Full Length Article

Fine-Grained Two-Factor Access-On Cloud Deployment

[a]S.Thiruvenkatasamy, [b]M. Santhosh, [b]M. Aparna, [b]A. Shalinipriya

[a]*Assistant Professor, Department of Computer Science and Engineering, Nandha College of Technology, Erode- 638052, Tamilnadu, India*

[b]*Department of Computer Science and Engineering, Nandha College of Technology, Erode- 638052, Tamilnadu, India*

***Corresponding Author**
S.Thiruvenkatasamy
Tel: +91 9843307809
Received : 19-7-2017
Reviewed : 25-7-2017
Revised : 26-7-2017
Accepted : 05-8-2017

DOI:

ABSTRACT:

Despite of the many advantages of migrating enterprise important assets to the Cloud, there area unit challenges specifically associated with security and privacy. It is vital that Cloud Users perceive their security and privacy desires, supported their specific context and choose cloud model best suitable support these desires. The literature provides works that focus on discussing security and privacy issues for cloud systems but such works do not provide a thorough methodological approach to elicit security and privacy necessities neither ways to pick cloud readying models supported satisfaction of those necessities by Cloud Service suppliers. This work advances this state of the art towards this direction. In specific, we have a tendency to contemplate necessities engineering ideas to elicit and analyze security and privacy necessities and their associated mechanisms employing a abstract framework and a scientific method. The work introduces assurance as proof for satisfying the safety and privacy necessities in terms of completeness and reportable of security incident through audit. This allows perspective cloud users to outline their assurance necessities so acceptable cloud models may be designated for a given context. To demonstrate our work, we tend to gift results from a true case study supported the Greek National Gazette.

Keywords: Cloud Computing; Cloud Security; Cloud Deployment model.

1 Introduction

Migrating into the cloud certainly gives an organization tangible competitive advantages due to significant cost savings, improved degree of scalability, flexibility and resource pooling availability. Moreover, organizations can take advantage of Infrastructure, Platform or Software as a Service deployment models and a range of service models to choose from – Public, Private, Hybrid and Community. However, there are many uncertainties about the migration process, specifically related to the dependency of an outside provider for the existing business model, data usage and leakage, lack of understanding about the cloud. Security and privacy are major concerns for organizations, which hinder cloud adaption as migrating into the cloud means organizations need to store their sensitive electronic assets into the providers' infrastructure. Existing business applications and data are mostly controlled through the provider's infrastructure depending on the chosen model, i.e. Saas, PaaS, IaaS, on which users may not have full/any control. Users' data are generally stored in a multi-tenant platform. This scenario introduces extra security and privacy challenges satisfaction of the requirements through audit and comparing to the traditional computing environment monitoring facility of user data incurs less user confidence on cloud based systems. Techniques to analyze the security and privacy issues in the context of cloud computing are different to those provided by the existing literature for traditional computing environments. It is therefore necessary to develop methods that not only identify and analyse security and privacy requirements but also provide certain assurance that these requirements are met by a specific cloud model before undertaking the migration decision. While such initiative have been put in place in for traditional IT based systems, the literature fails to provide evidence of a framework that fulfils that objective for cloud based services. This paper provides work towards this direction. The novelty of the presented work is twofold. Firstly, it contributes to the current state of the art by providing a modelling framework that supports the elicitation and analysis of security and privacy needs, and a cloud migration process for the selection of an appropriate cloud model. Secondly, it introduces assurance requirements in the proposed transparency. This allows us on one hand to identify and

analyze GR-security and privacy requirements and on the other hand to verify whether a chosen cloud deployment model addresses the identified requirements with appropriate mechanisms based on a specific organizational context.

2 MODULE DESCRIPTION

2.1 Cloud Setup Module

This module enhances the schemes which allow multi-keyword query and provide result similarity ranking for effective data retrieval, returning undifferentiated results. Privacy-Preserving: to stop the cloud server from learning further info from the dataset and therefore the index, and to satisfy privacy. Efficiency: Goal son functionality and privacy should be achieved with low communication and computation over head.

2.2 Pre-filtering And Security Management Module

This module is employed to assist the user to urge the correct result supported the multiple keyword ideas. The users will enter the multiple words question, the server goes to separate that question into one word once search that word come in our info. Finally, pre-filter the matched word list from the database and the user gets the file from that list. The search query is also described as a binary vector association rule each bit means whether corresponding keyword appears in this search request. The similarity can be precisely measured by dot product of question vector with information vector.

2.3 Encrypt Module

This module is used to help the server to encrypt the document using TRIPLE DES Algorithm and to convert the encrypted document to the Zip file with activation code and then activation code send to the user for transfer.

2.4 Client Module

This module is employed to assist the consumer to look the file victimisation the multiple key words conception and acquire the correct result list supported the user question. The user goes to pick out the desired file and register the user details and acquire activation code in mail from the“customerservice404” email before enter the activation code. After user will transfer the zip file and extract that file.

2.5 Multi-keyword Module

This module is employed to assist the user to urge the correct result supported the multiple keyword ideas. The users will enter the multiple words question, the server goes to separate that question into one word when search that word get into our information. Finally, show the matched glossary from the information and also the user gets the file from that list. The search question is additionally represented as a binary vector wherever every bit means that whether or not corresponding keyword seems during this search request, therefore the similarity may well be precisely measured by scalar product of question vector with knowledge vector. HoItver, directly outsourcing data vector or query vector will violate index privacy or search privacy. To meet the challenge of supporting such multi-keyword linguistics whereas not privacy breaches, It propose a basic SMS theme practice secure inner product computation, that is tailored from a secure k-nearest neighbour (kNN) technique, then improve it step by step to realize numerous privacy needs in 2 levels of threat models.

2.6 Admin Module

This module is employed to assist the server to look at details and transfer files with the safety. Admin uses the log key to the login time. Before the admin logout, change the log key. The admin will amendment the watchword once the login and consider the user downloading details and also the count of file request details on flow diagram. The admin will transfer the file once the conversion of the zip file format.

2.7 File Upload Module

This module is employed to assist the server to look at details and transfer files with the safety. Admin uses the log key to the login time. Before the admin logout, change the log key. The admin will amendment the watchword once the login and consider the user downloading details and also the count of file request details on flow diagram. The admin will transfer the file once the conversion of the zip file format.

3.Conclusions

Cloud migration is one of the most important concerns nowadays for both private and public organisations since due to the recent financial situations every organisation is aiming on cost reductions without losing efficiency and service quality. However, before migrating services, data or infrastructure into the cloud, it is necessary to realise and understand the migration needs and risks that cloud migration hinders. These risks vary among organisations especially due to the variability of information as well as the type of cloud services each organization wishes to use. Finally, the selection of the respective cloud model that

will be adopted plays an important role on the potential risks that the organization might face as well. Thus, the role of security and privacy are very important for an organization to decide which cloud solution fits best its needs and requirements. In this paper, a framework for supporting the elicitation and analysis of organisation's security and privacy needs and assurance to support these needs are presented. The aim of the framework is to assist organisations in selecting the most appropriate cloud model based on their security and privacy needs. We consider security and privacy requirements engineering concepts for the proper elicitation and analysis of the requirements and include assurance requirements for verifying the fulfil of the requirements using completeness, auditable and reportable metrics. By quantifying the fulfil of every suggested cloud model it is easier and more efficient to suggest the solution that should fit on the specific organisation's context and security and privacy goals. Finally, the applicability of the proposed framework was demonstrated on a real case scenario. The study results show that the approach supports the understanding of security and privacy requirements from the studied organisational context and identifies possible deployment scenarios so that appropriate decision can be taken. The assurance confirms which deployment model is suitable for the context. We plan to develop tool support to automate the elicitation and assurance activity. We would also like to focus on in-depth analysis of business issues and existing CSP offers.

References

[1] Pd.J. Bruening, and B.C. Treacy "Privacy & Security Law Report: Privacy", Security Issues Raised by Cloud Computing. The Bureau of National Affairs, 2009

[2] M. Ouedraogo and H. Mouratidis "Selecting a cloud service provider in the age of cybercrime", Computers & Security, Special issue on Cybercrime in the Digital Economy, vol.38, pp.3-13, Elsevier, 2013

[3] P.G. Dorey and A. Leite "Commentary: Cloud computing – A security problem or solution?" Information Security Technical Report, vol. 16, no. 3-4, pp. 89-96, Elsevier, 2011AICPA "Statement on Auditing Standards (SAS) n°70", from http://sas70.com/sas70_overview.html, 2012

[4] NIST, US Government Cloud Computing Technology Roadmap Volume II Release 1.0 (Draft), Useful Information for Cloud Adopters, November 2011CSA, Cloud Controls Matrix V.3.0.1,2014,https://cloudsecurityalliance.org/research/ccm/

[5] M. Ouedraogo, E. Dubois, D. Khadraoui, S. Poggi and B. Chenal "Adopting an Agent and Event Driven Approach for Enabling Mutual Auditability and Security Transparency in Cloud Based Services, In Proceeding of CLOSER 2015