International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 4
April 2017

Establishing Cloud Computing Security in trust-based Cloud Service Provider

Prof. Dhanashri Patil
Department of Computer Engineering
Pillai HOC College of Engineering and Technology, Rasayani

Ms. Pranita Patil
B.E Student
Pillai HOC College of Engineering andTechnology, Rasayani

Ms. Priyanka Patil
B.E Student
Pillai HOC College of Engineering and Technology,Rasayani

ABSTRACT

In cloud service environments, the quality of service levels is important to customers. Client's use cloud services to store, backup, recover and process data. If customer loss their data because of many reason, the customer's business may get affected. Therefore it is big challenge for a client to select an appropriate cloud service provider to ensure guaranteed service quality. To support customer's in reliably identifying cloud service provider, this work offer a framework selection of cloud service providers(SCSP), which involve trustworthiness, competence to estimate risk of interaction, data backup and data recovery. Trustworthiness is obtained from feedbacks related to reputations of service providers. Competence is computed based on transparency in provider's service. This work proposes a case study that has been presented to describe the application of our approach.

Keywords: Cloud Service provider, Trust, Data recovery, Data backup, Performance risk, Competence, Control, Transparency

.

I. INTRODUCTION

Cloud computing offers better resource utilization by multiplexing the same physical resource among several tenants. Users does not have to manage and maintain servers and in turn, uses the resources of cloud provider as services. For any service, a cloud customer may have multiple service providers. challenge lies in selecting an "appropriate" service provider among them. By the term ideal, we imply that a service provider is trustworthy as well as competent. Selection of an cloud service provider is non-trivial because a customer uses third-party cloud services to serve its clients in cost effective and efficient manner. Data loss owing to provider's incompetence or malicious intent can never be replaced by service credits. In the present work we focus on selection of a trustworthiness, risk estimation, data backup and data recovery.

II. BASIC SCHEM

A.Cloud Model:

In the below figure we prepared model in which client, cloud service provider (CSP)cloud server and Remote data backup center.cloud user is who stores large Quantity of data or files on a cloud server. Cloud server is a place where we are storing cloud data and that will be manage by cloud service provider

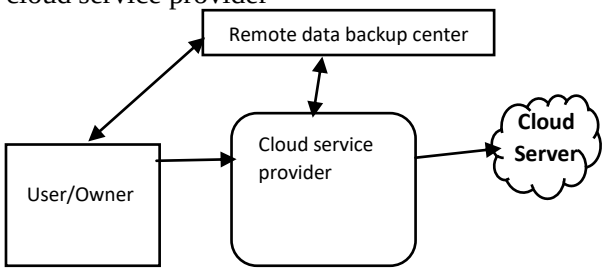

Fig1. "Cloud data storage"

The propose system user can upload their data in cloud and all the data uploaded by user is uploaded in encrypted form.User can share data only those persons who are member of cloud service as well as user can share the data by creating group of respective members. Proposed system consist watermark technique to find data leaker. Remote data backup center recover the files in case of the file deletion or if the cloud gets destroyed due to any reason.

B.Remote data backup center:

The backup of main cloud is nothing but the copy of main cloud. When this server is remotely located and they having complete copy of main cloud, then this remotely located center called as Remote Data Backup center where as main cloud known as central repository and remote cloud known as remote repository.In case of central repository lost its data in some situations or that can be happen by human attack like file deletion at that time it uses the data store in remote repository.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 4
April 2017

The main purpose of remote backup centre is to collect the information from only remote location and or data not found in main cloud.

III. EXISTING SYSTEM

•No work addresses the issue of selecting trustworthy service provider in cloud marketplace.
•Risk estimation of outsourcing a business onto third party cloud has not been handled in reported works.
•Models proposed in reported works lack experimentation and analysis.
• Models proposed in reported works lack backup and recovery system.
• security issues.

IV. PROPOSED MODEL

The main aim of developing a framework, called scsp, selecting an ideal cloud service provider for business outsourcing. SCSP framework provides APIs through which both customers and providers can register themselves. We make sure that only registered customers can provide feedbacks and they do not have any malicious intents of submitting unfair ratings. Various modules constituting the framework are as follows:

1) Risk Estimate: It computes perceived interaction risk relevant to a customer-CSP interaction by combining trustworthiness and competence.
2) Trust Estimate: It estimates trust between a customer CSP pair provided direct interaction has occurred between them.
3) Reputation Estimate: It evaluates reputation of a CSP based on feedbacks from various sources and computes the belief a customer has on former's reputation.
4) Trustworthiness Computation: Function to evaluate a customer's trust on a given CSP.
5) Competence Estimate: It estimates competence of a CSP based on the information available from its SLA.
6) Risk Computation: It computes perceived interaction risk relevant to a customer-CSP interaction.
7) Interaction ratings: It is a data repository where customer provides feedback/ratings for CSP.

V. ALGORITHM

A. Blowfish Algorithm

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time. it will follows the feistel network and this algorithm is divided into two parts.

1. Key-expansion
2. Data Encryption

B. Seed Block algorithm

The Seed Block Algorithm works to provide the simple Back-up and recovery process. It consists of the Main Cloud, its clients and the Remote Server.

VI. WORKING OF PROJECT

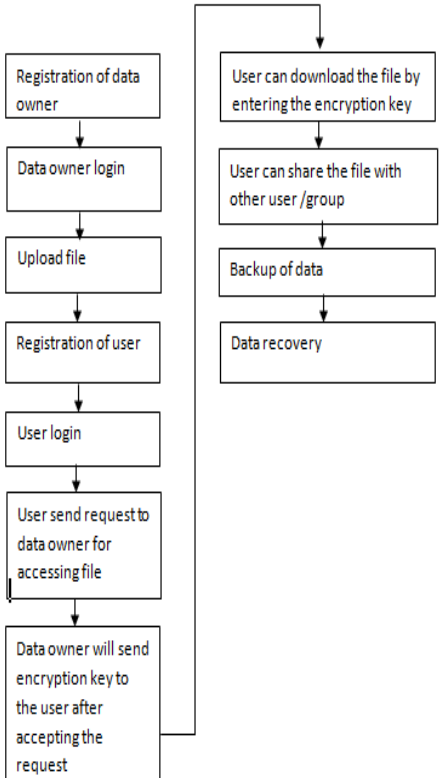

Fig2. "Working of Model"

CONCLUSION

In cloud computing one of the challenge for a cloud customer is how to select an appropriate service provider from the cloud marketplace to complete its business needs. Customers use cloud services to store their individual client's data, recover data and process it. Guarantees related to service quality level is of very important. For this

purpose, it is important from a customer's point of view to establish trust relationship with a provider. In this project, we propose a framework SCSP, which facilitates selection of trustworthy and competent service provider. The framework compute trustworthiness in terms of context-specific, dynamic trust and reputation feedbacks. Such estimations help customer to select appropriate service provider. In this work we propose backup and recovery, service management and storage. Results establish validity and efficacy of the approach with respect to cloud computing realistic scenarios.

REFERENCES

[1]Nirnay Ghosh, Student Member, IEEE, Soumya K. Ghosh, Member, IEEE, and Sajal K. Das, Senior Member, IEEE, "SelCSP: A Framework to Facilitate Selection of Cloud Service Providers", IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL.3,NO.1, JANUARY-MARCH 2015.

[2] S. K. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011, spp.933–939, i:10.1109/TrustCom.2011.129.

[3] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing," IT Professional, IEEE Journals & Magazines, vol. 12, no. 5, pp. 20–27, October 2010, doi: 10.1109/MITP.2010.128.

[4] J. Lin, C. Chen, and J. Chang, "Qos-aware data replication for data intensive applications in cloud computing systems," IEEE Transactions on Cloud Computing, vol. 1, no. 1, pp. 101–115, January-June 2013.

[5] A. Jøsang and S. L. Presti, "Analysing the relationship between risk and trust," in Second InternationaZl Conference on Trust Management, T. Dimitrakos, Ed., Oxford, March 2004.

[6] T. Grandison and M. Sloman, "A survey of trust in internet applications," IEEE Communications Surveys and Tutorials, vol. 3, 2000.