ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

A Framework To Ensure Secure Risk Based Cloud Service Providers

P.GRACY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
M.KUMARASAMY COLLEGE OF ENGINEERING
KARUR
Gracejosh169@gmail.com
7708986520

Asst Prof Mr. R.VIKRAM M.E.,
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
M.KUMARASAMY COLLEGE OF ENGINEERING
KARUR
Vikramr.cse@mkce.ac.in
7812836698

*Abstract:-***Cloud computing is transforming the IT industry to offer access to their support and operation. Due to the vast variety in the available Cloud services, it has become difficult to choose whose services they should use. By ranking method service provider can be easily choosen, but there is risk. To avoid risk service level agreement (SLA) is used. Even though service level agreement (SLA) provide quality of services, customers does not get satisfied. In cloud, customers use third party cloud service to store their clients data. So there is a chance of losing data. To avoid loss of data and to choose an ideal service provider, SelCSP a framework has been proposed. It combines trustworthiness and competence to calculate risk of interaction between customer and provider. Trustworthiness can be known from the personal experience of customers. Whereas competence can be known from the providers transparency in SLA. So we need to study the inter-relationships between trust, competence and risk. Though there is a risk in choosing cloud service providers, security is ensured to critical data by collaborating multiple domain in cloud environment.**

INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers.

Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach helps maximize the use of computing power while reducing the overall cost of resources by using less power, air conditioning, rack space, etc. to maintain the system. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.

IaaS refers to online services that abstract user from the detail of infrastucture like physical computing resources, location, data partitioning, scaling, security, backup etc.

PaaS vendors offers a development environment to application developers. The provider typically develops toolkit and standards for development and channels for distribution and payment. In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming-language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers.

In the software as a service (SaaS) model, users gain access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis or using

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

a subscription fee.

Trust is one of the main obstacle for the growth of cloud computing. Protecting private data of an organization plays an important role. An organization consist of critical data. Main motto of an organization is to protect the critical data. So the organization delegate data to the cloud to provide security and organization delegate data to the cloud to provide security and their data. So there is a chance of losing data. To prevent the data which is outsourced on the public cloud, a key management is required. Outsourced data should be encrypted. So that unauthorized users can not access data. An ID management is required to identify authorized users. Cloud service provider may have different levels and quality of services.

To know the quality of services ranking method is used. Based upon the feedbacks given by the users who have received services from those service providers. Credibility method is used to find whether the given feedback is malicious feedback (or) trustworthy feedback. If a cloud service provider satisfy the criteria of Service Level Agreement (SLA), then it provide quality of services. Even though it provide services with similar functionalities, users does not get satisfied with it. A framework is implemented to choose an appropriate service provider.

By choosing an appropriate cloud service provider we can avoid loss of data and cost. Quality, level, performance etc of a cloud service provider can be known easily. A framework which provides secure risk based cloud service provider.

1.2 SELCSP FRAMEWORK

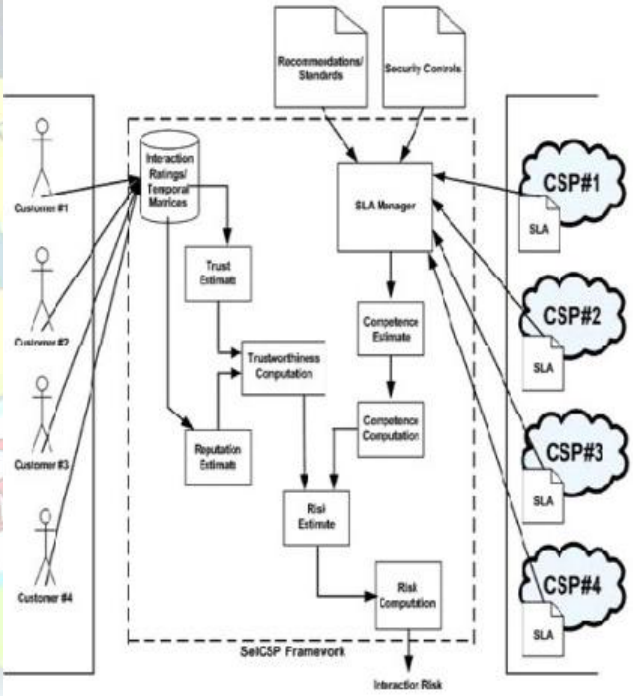
In this framework customer and provider both will register. Where customer will provide ratings of the cloud service providers whom they have already received services and also provide feedbacks. Cloud service provider will register in Service Level Agreement (SLA). Each cloud service provider consist of SLA. Cloud service provider can provide security only when it satisfies the criteria of those SLA's.

There is a Service Level Agreement manager which manages all SLA's. Based upon the trustworthiness and competence provided by the customer and service provider, performance of the provider can be known.

In cloud marketplace, vendors negotiate service quality levels with customers by means of SLA. Different vendors offer different SLA structures, service offerings, performance levels, and negotiation opportunities. SLA can be used to select a service provider on the basis of data protection, continuity, and cost.

Service qualities which provider guarantees to offer through SLA are measured by some metrics based on which its monitoring and auditing may be done. These metrics are known as SLA parameters. Each high-level SLA parameter is a function of one or more key performance indicators (KPIs) . SLA helps to generate trust relationship among customers and providers.

Majority of cloud service providers guarantee "availability" of service. However, other than "availability" there exists other SLA parameters whose inclusion is necessary to render completeness to any SLA. This is because, consumers not only demand availability guarantee but also other performance related assurances which are equally business critical. SelCSP recommends a provider with whom the risk of interaction is minimum.



LITERATURE REVIEW

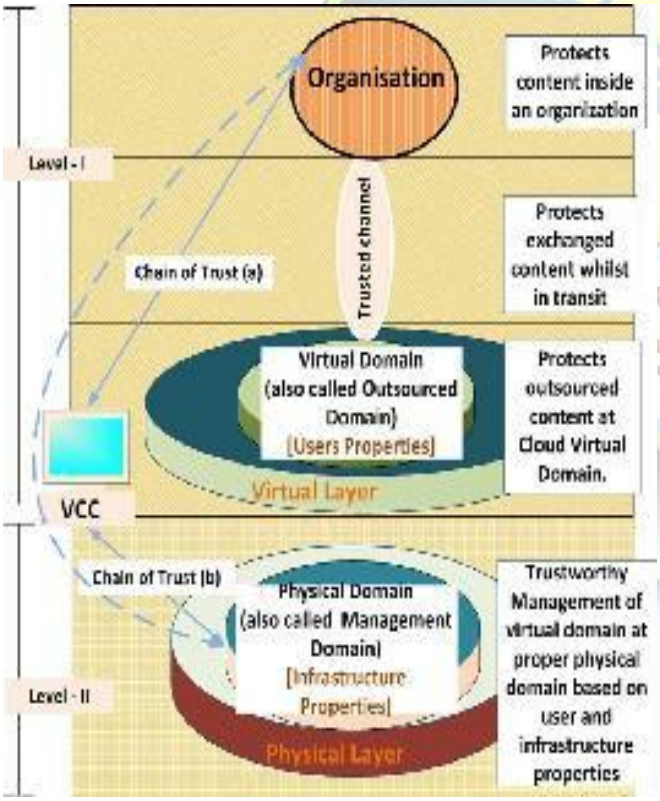
A.SECURITY AWARE CLOUD

In cloud security is the main problem. Particularly protecting private data which is outsourced by an organization. Three problems take place when an organization delegate its data to cloud. Multi stack holder problem, open space security problem, critical data handling problem. First two problems are solved by security aware cloud. Where the third problem requires an organization itself to build a private cloud. Middle size organization are unable to carry out the process.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

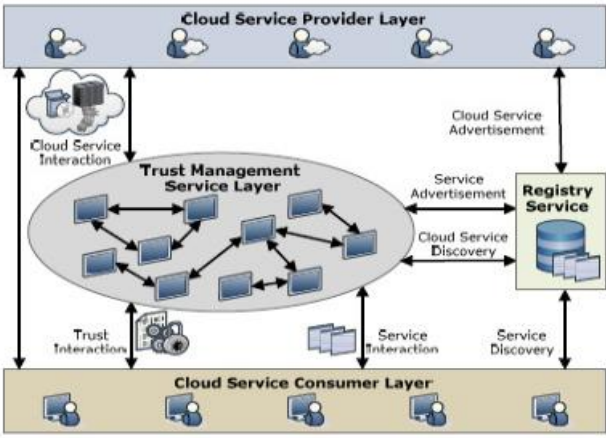
B.ESTABLISHING TRUST IN CLOUD

Two kinds of layers are used to establish trust in cloud to provide security to critical data. Horizontal layer and vertical layer. Horizontal layers are physical, virtual, application layer. Vertical layers are server, network and storage layer. Each Horizontal Layer contains Domains. Physical Domains, Virtual Domains and Application Domains. Domains at physical layer are related to cloud infrastructure. Other two layers are associated with cloud user properties. By establishing trust in cloud we can manage and maintain data and can provide security but it is very complex to establish trust.



C.TRUST AS A SERVICE

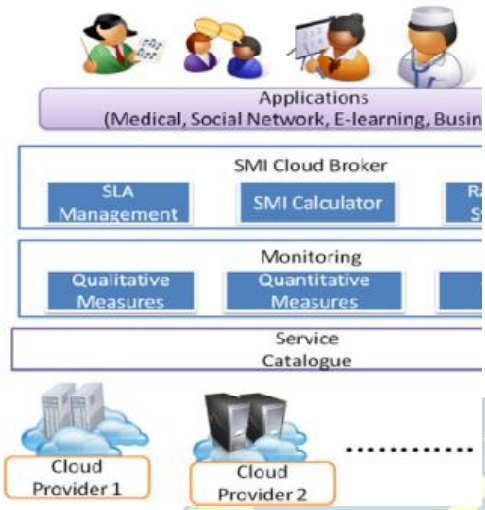
Only by receiving the feedback user can trust the service Providers. Trustworthy feedback and malicious feedback Can be separated only by credibility method. This method Consists of two analysis. Analytical analysis and empirical analysis. Analytical analysis measure trust result accuracy. Whereas empirical analysis focus on trust result measurement. Trust Management Service (TMS) is used to manage the Services.



D.RANKING OF CLOUD COMPUTING SERVICES

Choosing the cloud service provider by its quality using a framework. Through the QoS requirements cloud service provider can be choosen. Ranking is done based upon comparison between service providers and providers too will be aware of other service providers service quality and performance. Ranking of cloud services reduce the cost of users and helps to improve the quality of service.(SMI) Service Measurement Index used to measure the standard of services by comparison.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016



EXISTING SYSTEM

SelCSP framework provides APIs through which both customers and providers can register themselves. After registering, customer can provide trust ratings based on inter-actions with provider. Cloud provider needs to submit its SLA to compute competence. We assume that only registered customers can provide referrals/feedbacks and they do not have any malicious intents of submitting unfair ratings.
Various modules constituting the framework are as follows:

3.1 RISK ESTIMATE

It estimates perceived interaction risk relevant to a customer-CSP interaction by combining trustworthiness and competence.
$R = Rr + Rp$
Rr denotes relational risk and Rp is performance risk.

3.1.1 Relational risk

It is defined as the probability and consequence of not having satisfactory cooperation.
This risk arises because of potential opportunistic behaviour on part of both stakeholders (consumer and provider).

$$Rr(c_j,p_k) \propto 1 / T(c_j, p_k)$$

where, c_j is jth customer who wishes to interact with kth cloud service provider p_k, T
(c_j, p_k) is the trust which c_j has on p_k.

3.1.2 Performance risk

It is defined as the probability and consequences that alliance objectives are not achieved despite satisfactory cooperation among the partner firms.

$$Rp(c_j , p_k) \propto 1 / C(p_k)$$

where $C(p_k)$ is the competence of provider p_k.

$$R(c_j, p_k) = k1.1/ T(c_j , p_k) + k2.1/ C(p_k)$$

3.2 TRUST ESTIMATE

It computes trust between a customer-CSP pair provided direct interaction has occurred between them.

- **Temporal window**

Trust associated with an entity is dynamic and changes over time. For trust calculation, interactions which have taken place within a predefined time window will only be taken into consideration. Time is an intrinsic variable and can be denoted with an ordered discrete set τ of time values, such that,

$$t_i \in \tau, i \in N, t_{i-1} < t_i$$

- **Context**

Context defines the scope of interaction between provider/consumer agents. It refers to services which are offered by cloud provider. These services are used by customers to accomplish their tasks. Based on the type of cloud service delivery model, context of interaction will vary.
Some contexts specific to different service delivery models.

Infrastructure-as-a-Service (IaaS)
Backup and recovery, instances for computation, content delivery networks (CDN), service management, storage.
Platform-as-a-Service (PaaS)
Development environment, database, testing integration, deployment.
Software-as-a-Service (SaaS)
Email and office suite, collaboration, customer relation management (CRM), document management, social networks enterprise resource planning (ERP).
Each of these contexts may be having multiple granular sub contexts on which cloud based interactions may take place.

- **Trust domain**

Trust domain contains five qualitative elements or states of trustworthiness:
distrusted(D), partially distrusted (PD), undecided (U), partially trusted (PT), and trusted(T).
The respective quantitative ratings lie in the closed interval

$$[0,2]:D=\{0,0.5,1.0,1.5,2.0\}$$

- **History of interaction**

A history of interaction H on any context α_i observed during the temporal window τ with time values, will have cardinality $|H|=N$ and is given by a set

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

of ratings $\delta_1, \delta_2, \ldots \delta_N$, such that for all $\delta_i \in H: \delta_i \rightarrow D$.

For each customer, SelCSP framework maintains an interaction matrix I. It contains trust scores computed from ratings assigned by the customer to different providers for interactions occurring over various contexts.

3.3 REPUTATION ESTIMATE

It evaluates reputation of a CSP based on referrals/feedbacks from various sources and computes the belief a customer has on former's reputation. Reputation model comes into effect when customer c_j has not interacted with provider p_k on current context in the past. Under this situation, c_j has to believe in feedbacks/referrals from other customers who have directly interacted with p_k. We denote a customer providing feedback as a"witness" from c_j's viewpoint. Feedbacks from various witnesses are to be combined to obtain a global reputation score for any provider. Dempster-Shafer belief model defines a set of possible situations which is called the frame of discernment. If Θ is the frame of discernment, then the power set $2^{|\Theta|}$ contains the elementary/atomic sets and all possible union of atomic sets, including Θ.

- **State-based belief**
  It is the belief which c_j has on a given state of trustworthiness with respect to p_k's reputation.
- **General belief**
  It is the overall belief that c_j has towards p_k's global reputation.

3.3.1 State-based reputation vector

Given a customer c_j that wants to compute the reputation of a provider p_k, a state-based reputation vector model SREPUTE is a four tuple SREPUTE = (S, d_i, D, ξ), where S is a function that evaluates belief and disbelief measures, d_i is the state from the trust domain D under consideration, and ξ is a function to evaluate the state-based reputation vector.

3.3.2 Aggregated reputation vector

Given a customer c_j that wants to compute the reputation of a provider p_k, an aggregated reputation vector model AREPUTE is a three tuple AREPUTE = (R, D, π), where R is a set of state-based reputation vectors for states in D, and π is a function that evaluates the overall reputation vector.

3.4 TRUSTWORTHINESS COMPUTATION

Function to evaluate a customer's trust on a give CSP. Given a customer cj that wants to make decision regarding initiation of an interaction with a service provider pk, a trust and competence based risk estimator TCRISK is a seven-tuple TCRISK= (α, I, U, T, C, Φ, R) where, α is the current context of interaction, I is the importance of the context subjective to c_j, U is the utility expected to be gained on context α by c_j,T is the degree of trustworthiness obtained by c_j towards p_k on context α, C is competence of p_k with respect to present SLA, Φ and R is a function to evaluate the perceived interaction risk.

3.5 SLA MANAGER

This module manages SLAs from different CSPs. It takes into account different recom-mendations/standards and controls which are supposed to be satisfied by the SLAs.

3.6 COMPETENCE ESTIMATE

It estimates competence of a CSP based on the information available from its SLA.Service qualities which provider guarantees to offer through SLA are measured by some metrics based on which its monitoring and auditing may be done. These metrics are known as SLA parameters. Each high-level SLA parameter is a function of one or more key performance indicators (KPIs) which are composed, aggregated, or converted to form the former. Based on the QoS+ parameters proposed in conjuncture with Cloud Controls Matrix (CCM). In SelCSP, we assign three qualitative attributes: high,moderate, and low, to denote transparency of controls. 1.0 for high, 0.5 for moderate, and 0.1 for low. Overall competence (C) of a service provider pk in terms of any SLA Φ is the mean of aggregated transparencies of all parameters.

$$C(p_k,\Phi) = 1/n \sum_{i=1}^{n} \lambda_{\text{param i}}(\Phi)$$

3.7 COMPETENCE COMPUTATION

It computes transparency with respect to a given SLA and hence evaluates the competence of the CSP.

3.8 RISK COMPUTATION

It computes perceived interaction risk relevant to a customer-CSP interaction.

3.9 INTERACTION RATINGS

It is a data repository where customer provides feedback/ratings for CSP.

PROBLEM DESCRIPTION

SelCSP framework which combines trustworthiness and competence to evaluate risk of interaction between customer and provider. And also to identify ideal service provider to get a quality and secured service to protect the data which is stored in cloud. Though Service Level Agreement (SLA)

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

which guarantee quality of services are not satisfied by providers even though they provide services with similar functionalities. SLA is used to choose the service provider on the basis of data protection, continuity, cost. Due to the lacking of quality in services, there is a chance to loss data

which is stored in cloud.

Loss of data can be reduced by evaluating risk of interaction between customer and provider.

To calculate interaction risk trustworthiness and competence should be known.

In SelCSP framework both customer and provider should register at first. Customers want to register at interaction rating. Registering is nothing but customers will provide feedback (or) ratings about the service providers whom they have already received services. Customers who provide feedback are the one who have already received services from those providers. Customers who provide ratings doesn't know about the service providers they provide ratings based on other customers feedback about the providers. Each cloud service provider consist of an SLA. Those cloud service providers who meet the conditions of an SLA, can register in SLA manager.

Trustworthiness can be known from customers feedback and competence can be known from SLA manager.

When both gets combined risk is evaluated. During risk computation interaction risk arises. Here various parameters are used to evaluate risk, trustworthiness and competence. A casestudy has been described which combines risk, trust and competence.

PROPOSED SYSTEM

5.1 INTRODUCTION

Choosing an appropriate cloud service providers can reduce cost, improve quality and performance. Here we are going to choose an ideal service provider to avoid loss of critical data by collaborating multiple domain in cloud environment. There is a risk in choosing ideal service provider at the same time security is provided to protect the critical data which is stored in third party cloud services. With the help of case study, graphs are drawn which provide a clear view about risk, trustworthiness and competence of each service providers separately. Based upon the case study an ideal service provider can be choosen easily and at the same time critical data which is stored in cloud will also be protected.

A virtual storage cloud system called DepSky which consists of a combination of different clouds to build a cloud-of-clouds. The DepSky system addresses the availability and the confidentiality of data in their storage system by using multi-cloud providers,combining Byzantine quorum system protocols, cryptographic secret sharing and erasure codes. DepSky algorithm exists in the clients' machines as a software library to communicate with each cloud. DepSky system deals with different cloud providers. The DepSky library permits reading and writing operations with the storage cloud. DepSky

Library deals with different cloud interface providers

and consequently, the data format is accepted by each

cloud.

5.2 CLOUD STORAGE PROVIDERS IN THE DEPSKY SYSTEM MODEL

The Byzantine protocols involve a set of storage clouds (n) where n = 3 f +1, and f is maximum number of clouds which could be faulty. In addition, any subset of (n – f) storage cloud creates byzantine quorum protocols.

5.3 ANALYSIS OF MULTI-CLOUD

Moving from single clouds or inner-clouds to multiclouds is reasonable and important for many reasons. Deals with multiple versions of data. It guarantee data confidentiality. Vendor lock-in is not needed. Proofs of Retrievability (PORs) and Proofs of Data Possession (PDP) are protocols used to ensure data integrity. By storing data on several clouds we can avoid loss of availability of service.

5.4 CRYPTOGRAPHIC METHOD

It is used to protect stored data in cloud using hash function. DepSky system stores the cryptographic keys in the cloud by using the secret sharing algorithm to hide the value of the keys from a malicious insider. In the DepSky system, data is replicated in four commercial storage clouds. Storing half the amount of data in each cloud in the DepSky system is achieved by the use of erasure codes.

5.5 BYZANTINE QUORUM SYSTEM PROTOCOLS

Implement read and write operation in the system, so it needs only two communication round

trips for each operation to deal with several clouds.

Byzantine fault-tolerant replication to store data on

several cloud servers, so if one of the cloud providers

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

is damaged, they are still able to retrieve data correctly.

5.6 SECRET SHARING ALGORITHM

This framework will apply multi-clouds and the secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity.

5.7 METHODOLOGY USED

DepSky provides security and service availability by combining

- Byzantine quorum system protocol
- Secret sharing algorithm
- Cryptography

ACKNOWLEDGEMENT

I owe my deep gratitude to my respected guide Asst Prof. Mr. R.VIKRAM who gives me the valuable guidelines with a touch of inspiration and motivation to progress my way through quite substantial barrier between early problem statement and something that resembled a fine work.

CONCLUSION

Choosing an ideal service provider is a critical problem, Though ranking is provided to cloud service providers. SelCSP, which facilitates selection of trustworthy and competent service provider. An estimate of risk level involved in interaction, enables a customer to make decisions regarding choosing a service provider and providing security to critical data which is stored in third party cloud service. A framework which estimate trustworthiness, competence and risk. Through this research we conclude that by combining service provider framework and DepSky method, we can provide security to the sensitive critical data and also avoid loss of service availability, quality and cost. A case study has been described and analysed to provide secure risk based cloud service provider by collaborating multi domain in cloud environment.

REFERENCES

[1] H. Sato, A. Kanai, and S. Tanimoto, "*A cloud trust model in a security aware cloud*," in Proc. 10th IEEE/IPSJ Int. Symp. Appl. Internet, 2010, pp. 121–124.

[2] IM. Abbadi and M. Alawneh, "*A framework for establishing trust in the cloud*," Comput. Elect. Eng., vol. 38, pp. 1073–1087, 2012.

[3] T. Noor and Q. Sheng, "*Trust as a service: A framework for trust management in cloud environments*," inProc. 12th Int. Conf. Web Inf. Syst. Eng., 2011, pp. 314–321.

[4] S. K. Garg, S. Versteeg, and R. Buyya, "*A framework for ranking of cloud computing services*," Future Gener. Comput. Syst., vol. 29, no. 4, pp. 1012–1023, 2013.

[5] *SelCSP: A Framework to Facilitate Selection of Cloud Service Providers* Nirnay Ghosh, Soumya K. Ghosh, Sajal K. Das VOL. 3, NO. 1, 2015