PRIVACY PROTECTION FOR INTERCLOUD

Sruthy K S
Masters in Computer Science & Engineering
RCET, Akkikavu
chindu333@gmail.com

***Abstract*— InterCloud Platform is an application-aware platform giving non-public access to any cloud supplier, firmly and with efficiency delivering cloud applications where they will be needed. Intercloud seeks to facilitate resource sharing among clouds. To support Intercloud, a trust analysis framework among clouds and users is needed. For trust analysis, typical protocols unidirectional relationship. Here presents a distributed trust analysis protocol with privacy protection for Intercloud. The new contributions and innovative options are 1st, feedback is protected by homomorphic encoding with verifiable secret sharing. Second, to cater to the dynamic nature of Intercloud, trust analysis may be conducted during a distributed manner and is purposeful even once a number of the parties are offline. Third, to facilitate made-to-order trust analysis, associate innovative mechanism is employed to store feedback, such it may be processed flexibly whereas protective feedback privacy. The protocol has been tried supported a proper security model**

Index Terms— Intercloud ;Trust evaluation; cloud computing; Privacy; Reputation.

1. INTRODUCTION

With the rapid advancement of cloud computing, there is an increasing number of cloud services. Each provides different service qualities, pricing and access strategies. Choosing the right cloud services before actually using them is not trivial. In the conventional cloud computing environment, once a cloud user decides to select a cloud service, it is difficult and costly to switch to a new cloud service provider. To address this vendor lock in problem and to support more cooperative cloud services, Intercloud has been proposed. In the Intercloud paradigm, cloud service providers can process user requests by leveraging services from other clouds. Cloud service providers can share their infrastructure to improve overall resource utilization .Furthermore, applications can be migrated from one cloud service provider to another cloud service provider and workloads can be distributed among clouds for disaster recovery or multi-region application delivery .Here consider an Intercloud system based on the IEEE P2302 Draft Standard ,which employs a three tier architecture, namely, root exchanges and clouds. The root is a cluster of servers/clouds providing certification and naming services. The clouds provide cloud services to users and to each other.

2. GENERAL BACKGROUND

The basic Intercloud system can also be extended to support a mobile Intercloud system. In this case, heterogeneous clouds can work collaboratively under a mobile environment so that data, applications and virtual mobile terminals can move across clouds through various handoffs processes. In the Intercloud environment, cloud service selection can be made in an ad-hoc,dynamic and distributed manner. For instance, one cloud may want to select a number of reliable clouds to help run a time-consuming program. For mobile Intercloud, a mobile user may want to select a cost-effective cloud service in a foreign city. This makes cloud service selection in an Intercloud environment more challenging. The trustworthiness of cloud services is an important consideration for making cloud selection decision (i.e., knowing the expected performance of a cloud service). Currently, there has been little work done to study distributed trust evaluation for the Intercloud environment. It seeks to contribute to this important topic for the development of Intercloud. Trust in a service is generally concerned with a belief in whether the service can be delivered satisfactorily, in accordance with certain trust attributes. In the Intercloud context, a cloud service provider (or user) typically trusts another cloud service provider based on certain trust attributes, such as service reliability, quality of service and service efficiency. Before choosing/ using a service, trust evaluation is often conducted based on the feedback of existing users (i.e., reputation based trust evaluation). Indeed, feedback provided by past cloud users is a good reference for trust evaluation. Based on this feedback or rating, a cloud user can evaluate how likely (e.g., a probability) that a cloud service will be performed as expected. However, the credibility of feedback is often difficult to guarantee as cloud users often avoid leaving honest comments, especially negative ones. The main reason for this behavior is the unequal status between providers can easily remove negative comments about its services). This problem becomes more serious in the Intercloud environment. As there is more and more mutual co-operation, a cloud user or his/her business could be another type of cloud service provider in future business transactions. This possible mutual relationship makes the privacy requirement even more important in the Intercloud scenario. If feedback information cannot be made private, cloud users may only give positive feedback, as they want to maintain a good relationship or are fearful of retaliation. Hence, it is important to develop an effective and flexible trust evaluation protocol with privacy protection for Intercloud.

Cloud user protection. To encourage honest feedback/ ratings and to prevent possible retaliatory attacks, both user identity and user feedback privacy should be protected. Ideally, feedback should not be linked with the user and business privacy of the user (i.e., which user has performed business with which cloud service provider should not be disclosed). This protocol uses an innovative mechanism to store feedback, and employs homomorphism encryptions and with verifiable secrets haring to protect feedback privacy. Finally, neither the cloud service provider nor the enquirer can obtain individual feedback.

Cloud service provider protection. Malicious users can generate a large volume of misleading feedback or faked ratings to damage the reputation of a cloud service provider. To address this important issue, proposed protocol allows a cloud service provider to certify a rater's eligibility. Furthermore, as explained later, protocol allows the filtering of extreme ratings without leaking privacy information.

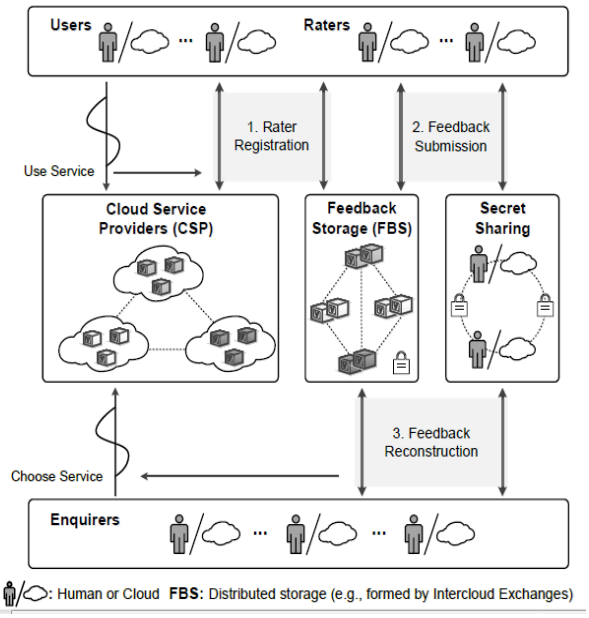
Trust result availability. Existing distributed protocols typically require all concerned parties to remain online to facilitate feedback collection. This requirement is not practical in the Intercloud environment. The proposed protocol can still function well, even if concerned parties are not available to contribute to trust evaluation.

Flexible processing of protected feedback. To facilitate customized trust evaluation and reduce the influence of misleading ratings, it is desirable to provide a flexible way to subjectively process protected feedback results.

Trust in a service is generally concerned with a belief in whether the service can be delivered satisfactorily, in accordance with certain trust attributes. In the Intercloud context, a cloud service provider (or user) typically trusts another cloud service provider based on certain trust attributes, such as service reliability, quality of service and service efficiency. Before choosing/using a service, trust evaluation is often conducted based on the feedback of existing users (i.e., reputation based trust evaluation). Indeed, feedback provided by past cloud users is a good reference for trust evaluation .Based on this feedback or rating, a cloud user can evaluate how likely (e.g., a probability) that a cloud service will be performed as expected. However, the credibility of feedback is often difficult to guarantee as cloud users often avoid leaving honest comments, especially negative ones . The main reason for this behavior is the unequal status between cloud service providers and cloud users (e.g., a cloud service provider can easily remove negative comments about its services). This problem becomes more serious in the intercloud environment. As there is more and more mutual co-operation, a cloud user or his/her business could be another type of cloud service provider in future business transactions. This possible mutual relationship makes the privacy requirement even more important in the intercloud scenario. If feedback information cannot be made private, cloud users may only give positive feedback, as they want to maintain a good relationship or are fearful of retaliation. Hence, it is important to develop an effective and flexible trust evaluation protocol with privacy protection for intercloud.

3. SYSTEM MODEL

Fig. 1 shows the system model or architecture with five main components: cloud service provider (CSP); user/rater; enquirer; distributed feedback storage (FBS) and secret sharing network. Under the Intercloud system model, the **CSP**s provide cloud services collaboratively to users, and serve each other as well. In general, there are two types of cloud service **users**: consumer users and business users. Consumer users use a cloud service. They have only a one-way trust/service relationship with a CSP (i.e., the service is one-way CSPs serving consumer users). Business users may provide services to each other (i.e., two-way trust/service relationship). After using a cloud service or under certain arrangements, the users can rate the service or a trust attribute (e.g., availability, response time, price, technical support). That means the users are also **raters** during the feedback/rating process.



Note that to facilitate the explanation, focus on evaluating one service or trust attribute. It can easily be extended to evaluate multiple services or trust attributes. For a business user, a human representative of the respective organization can provide the rating/feedback. Furthermore, with advances in intelligent computing technologies, a software agent or software robot can perform the feedback/rating task as well. These software agents/robots can communicate through Intercloud gateways (e.g., using an Intercloud communication protocol with predefined XML-based messages). In this case, the Intercloud system becomes a highly autonomous system. The enquirers can be any parties who want to use the trust evaluation protocol to evaluate the trustworthiness of a CSP based on the feedback/ratings.

4. SECURITY MODEL

An Intercloud trust evaluation protocol consists of rater registration, feedback submission and feedback reconstruction phases with relevant parties being the FBS, CSP, users/raters and enquirers. The specifications of the ideal-world system as follows:

Rater registration : Each user sends a request to register as a rater for a CSP to T, who forwards the request to the CSP concerned. The response from the CSP is sent back through T . Upon receiving approval, u sends another request to T for the registration as a rater with FBS. T first checks whether the request is legitimate, based on the CSP response. If the request is valid, T notifies FBS that one eligible user is requesting to give feedback for this particular CSP. Note that T will not reveal the identity of u to FBS. If FBS accepts this request creates a new rater identity r for u and informs u and FBS. FBS randomly groups raters together to obtain a set of raters. The set, R, is made known to all raters within the set through T.

Feedback Submission: Each rater sends a request to T for rater set R that includes r. T first checks whether the requester is rater r. Once it passes the check, T returns R to it. Rater acknowledges set R to T. T informs the FBS that rater r's R. After a period of time, each rater r submits its feedback f to T . Then, after T confirms the requester is rater r, it will store the feedback and inform FBS that rater r has submitted feedback, but without informing FBS about the content of the rater's rating choice.

Feedback Reconstruction: An enquirer asks T for the CSP feedback given by its past users. T forwards the enquirer's request to all raters in the R to ask whether they support the reconstruction of the feedback results. When there are a sufficient number of approval responses from raters, T calculates the sum of the feedback given by raters in the group R and returns this sum to the enquirer. Then T informs FBS that an enquirer has obtained the sum of the feedback in the group R.

5. REVIEW ON RECENT METHODOLOGIES

To conduct a review analysis and comparative study on "Privacy protection for intercloud" we have considered several recent studies on the topic.

Ana Juan Ferrer [1],here discussed about Inter-cloud Challenges, Expectations andIssues Cluster objective is to alter collaboration among European analysis comes addressing topics of multi-cloud and inter-cloud. Today this comes analyze the question from various views and that specialize in specific components of the matter. This position paper provides the work worn out collaboration by of these comes to outline analysis areas and challenges for 2020. It identifies a Cluster's vision of Inter-Cloud topics development by 2020, as well as, research areas in order to realize the provided vision. Inter-Cloud or Multi-Cloud is defined as the serial or simultaneous use of services from diverse providers to execute an application. At business level, Hybrid Cloud is the term commonly used, Gartner4 defines hybrid Cloud as the coordinated use of cloud services across isolation and provider boundaries among public, private and community service suppliers, or between internal and external cloud services. This simultaneous or serial use of services from diverse heterogeneous clouds is a challenge in order to further develop the Cloud market in Europe. While it presents a series of issues with regards to interoperability among heterogeneous cloud typologies, private and public clouds, services' comparability, portability, migration, networking, etc. It additionally offers innovative market opportunities for the event of recent roles within the cloud market associated with hybrid cloud models. Here reflects a part of the work conducted by the cluster that specialize in distinguishing Cluster's vision of Inter-Cloud topics development by 2020, as well as, identifying research areas and its prioritization so as to form the provided vision, reality. The cluster has done initial work in order to prioritize these identified Research Areas. The analysis has classified analysis areas consistent with Business Impact and Timeframe for realization. In addition, priority of the Research Area as a whole has been assessed based on priority of the associated challenges. This process has been performed by a survey completed by cluster participants. Details on analysis Areas and associated challenges are obtainable in Inter-cloud Challenges, Expectations and problems Cluster position. Findings of this analysis show that the area identified with major business impact in long term realization is Area Service Discovery and Composition, considering the automatic discovery and composition of cloud services at different levels and taking into account scalability, decentralization and automatization enabled by software defined everything. Although the expected business impact makes it feasible that market evolution alone will bring the realization of Area associated challenges, R&D investment would help European industry and research institutions to be well positioned for this expected market evolution.

A N Toosi, R N Calheiros and R Buyya [2], it's a brief review of the Internet history reveals the fact that the Internet evolved after the formation of primarily independent networks. Similarly, interconnected Clouds, also called Inter-Cloud, can be viewed as a natural evolution of Cloud computing. Recent studies show the advantages in utilizing multiple Clouds and gift attempts for the conclusion of Inter-Cloud or united Cloud atmosphere. However, Cloud vendors haven't taken into consideration Cloud ability problems and every Cloud comes with its own solution and interfaces for services. This survey initially discusses all the relevant aspects motivating Cloud interoperability. Furthermore, it categorizes and identifies possible Cloud interoperability scenarios and architectures. The spectrum of challenges and obstacles that the Inter-Cloud realization is Janus-faced with area unit lined, taxonomy of them is provided and fitting enablers that tackle each challenge are identified. All these aspects need a comprehensive review of the state of the art, including ongoing projects and studies in the area. Cloud computing is a

term used to describe a paradigm for delivery of computing services to users on pay-as-yo-go basis. In this paradigm, users utilize the Internet and remote data centers to run applications and store data. The Cloud technology permits additional economical computing by removing most of the direct prices of fitting associate IT infrastructure. It allows organizations to expand or reduce their computing facilities very quickly. There is an increasingly perceived vision that the birth of Cloud computing is a big step towards the long-held dream of computing as a utility Over the years, several technologies such as Virtualization, Grid computing, and Service-Oriented Architecture (SOA) have matured and significantly contributed to make Cloud computing viable. However, Cloud computing is still in its early stage and suffers from lack of standardization. What truly happens is that almost all of latest Cloud suppliers proposes its own answer and proprietary interfaces for access to resources and services. This heterogeneity is a crucial drawback because it raises barriers to the trail of the ever-present Cloud realization. The main barrier is vender lock-in that is ineluctable at this stage ; customers applying Cloud solutions have to be compelled to tailor their applications to suit the models and interfaces of the cloud supplier, which makes future relocation costly and difficult. Furthermore, Cloud computing, as a novel utility, requires ubiquitously interconnected infrastructure like other utilities such as electricity and telephony. Accordingly, ability and immovableness across Clouds area unit vital not just for protection of the user investments however conjointly for realization of computing as a utility.

6. Comparative Analysis And Discussion

In this section, compared the trust result accuracy of this protocol with the scheme that uses additive secret sharing (ASS). Clark and Hassan both used ASS in their schemes to protect feedback privacy. It simply adds all of the secret shares together. ASS requires all raters to stay online to enable the computation of trust results. When any rater leaves the network or refuses to reply, all corresponding feedback shares will be lost in the trust result, causing inaccurate trust results. To perform the analysis, let T r denote the trust result of each CSP computed from all of its raters. Let T r 0 denotes the trust result of each CSP computed from the raters who are not selfish. Consider the trust result accuracy as the average value T r 0 T r of all CSPs whose trust results can be recovered. In the subsequent simulations, randomly choose selfish raters 2 [5%; 50%], with an increment of 5% in the Advogato trust graph. Set m=n = v=n = 0:4 in our protocol and in ASS approach; such that the majority of feedback can be recovered. For the random graphs, we assume 50% selfish raters. Comparing the result of Random-a and Random-b, it can be seen that the network density p has more influence on the feedback recovery efficiency. When the network density p _ 10%, the enquirer needs more iterations to obtain the feedback sum (i.e., less efficient).

7. Conclusion And Discussion

In conclusion, presented a privacy protection for Intercloud. Compared to other protocols, this distributed protocol provides some distinctive features, particularly for the Intercloud environment. The first phase is rater registration was implemented with the FBS as a rater so that feedback/ratings on the service can be submitted. First, it supports user anonymity by means of blind signature, facilitating users to provide honest feedback without fear of a retaliatory attack. Second, by means of an innovative mechanism for storing feedback, feedback privacy can be protected by using homomorphic encryption with verifiable secret sharing. Third, it allows customized processing of evaluation results while protecting feedback privacy. A security model has been employed to evaluate the protocol for its effectiveness. Unlike many other distributed protocols, which only support static configuration, the protocol can still be effective when some of the parties are offline (i.e., supporting a dynamic configuration). Simulation results indicate the protocol can still function well when half of the parties are malicious or offline. Future work is being planned to further analyze and enhance the protocol(e.g., using distributed ledger technology). For example, various block chains can be formed(e.g., among Intercloud Exchanges, CSPs and users). It is of interest to study how the blockchains can interact to support trust evaluation and other advanced functions for Intercloud.

References

[1] A. J. Ferrer, “Inter-cloud research: Vision for 2020,” in 2nd International Conference on Cloud Forward: From Distributed to Complete Computing, Madrid, Spain, 18-20 October, 2016., 2016, pp. 140–143.

[2] A. N. Toosi, R. N. Calheiros, and R. Buyya, “Interconnected cloud computing environments: Challenges, taxonomy, and survey,” ACM Comput. Surv., vol. 47, no. 1, p. 7, 2014.

[3] E. Barlaskar, P. Kilpatrick, I. T. A. Spence, and D. S. Nikolopoulos, “Myminder: A user-centric decision making framework for intercloud migration,” in CLOSER 2017 - Proceedings of the 7th International Conference on Cloud Computing and Services Science, Porto, Portugal, April 24-26, 2017., 2017, pp. 560–567.

[4] T. Truong-Huu and C.-K. Tham, “A novel model for competition and cooperation among cloud providers,” IEEE Trans. on Cloud Computing., vol. 2, no. 3, pp. 251–265, 2014.

[5] L. Liu, S. Gu, D. Fu, M. Zhang, and R. Buyya, “A new multi objective evolutionary algorithm for inter-cloud service composition,”TIIS, vol. 12, no. 1, pp. 1–20, 2018.

[6] S. Sotiriadis, N. Bessis, A. Anjum, and R. Buyya, “An inter-cloud meta-scheduling (ICMS) simulation framework: Architecture and evaluation,” IEEE Trans. Services Computing, vol. 11, no. 1, pp. 5–19,2018.