A trust evaluation method based on the distributed Cloud Trust Protocol (CTP) and opinion sharing

Abdelmageed Algamdi, Frans Coenen and Alexei Lisitsa
Department of Computer Science
University of Liverpool
Liverpool, UK
(A.Algamdi - f.coenen - a.lisitsa)@liverpool.ac.uk

***Abstract*—In this paper we address the issue of trust in cloud computing. We propose a novel architecture for cloud trust management system in which various sources of trust related information are utilized and different trust mechanisms are combined. This includes using distributed Cloud Trust Protocol CTP), Consensus Assessment Initiative Questionnaire (CAIQ), trust aggregation and reputation mechanisms. Trust related information is presented and processed in terms of opinions formalized in subjective logic.**

Keywords-component; Digital trust; CTP; Opinion sharing; Subjective opinions; CAIQ assessment ;

I. Introduction

Over the recent years cloud computing has come to be considered an important technology, allowing users to remotely share the various resources over the internet. Through virtualisation and job scheduling, cloud computing can be employed in a unified manner. Despite the numerous advantages of using the cloud, cloud users may have some concerns regarding how to control their data and how to make sure that no one can access it except the owner. Another issue is availability, since online services, are bound to have downtime, and therefore data may not be available when the user needs them. Hence, trust needs to be built between the customers and the providers offering cloud services. Cloud trust management systems [1], [2], [3] are responsible for calculating the trustworthiness and finding the trustworthy ones. This is done based on trust and reputation models which translate the nature of different attributes such as data governance, compliance to the regulations, information security. Trust and reputation (TR) systems are example of how to build trust in various service environments. These systems provide TR models which are useful in decision making but most of them don't consider multiple attributes such as security, compliance and data governance [4].

The role of transparency was further acknowledged by the development of Cloud Trust Protocol (CTP) [6], [7]. CTP is a high-level protocol to achieve cloud providers' transparency by a query/response mechanism allowing the (potential) users to query providers about trust related information. Starting with the high-level specification [6], [7] the protocol has got very recently the proposed API [19] which brings it closer to the implementation stage.

Building upon these developments, in this paper we propose a novel architecture for cloud trust management system in which various sources of trust related information are utilized and different trust mechanisms are combined. This includes using distributed CTP, CAIQ, trust aggregation and reputation systems. This is done by using the trust information acquired by the CTP and the feedback of the users who already used services offered by the cloud service provider to assess the service quality using the CAIQ assessment.

We present an infrastructure for the system which provides with the capability to use the CTP, ask for assessments, calculate the digital trust for providers and ask for queries based on the stored trust values. This consumer assessment reflects the satisfaction of the user which have to be a main factor affecting the digital trust value. This will be achieved by using a MCQ questionnaire designed especially for the cloud consumer. The user opinion is extracted from the questionnaire answers using subjective logic operators AND and Consensus from [22], [23], [27] applied to *binomial opinions* represented by quadruples of real values, each within an interval [0…1]. Further subjective logic operators are used to aggregate the opinions of different users taking into account the timing of the assessments. Finally, the aggregated opinions are visualized using barycentric coordinates as points within a triangular area and depending on the sub-area they fall categorized into one of size classes: *very good, good, very bad, bad, unnamed* and *very uncertain.*

The rest of the paper is organised as follows: Section 2 reviews the related works and presents the background information related to our work. Section 3 and 4 demonstrate the suggested framework and the proposed assessment technique respectively. Section 5 concludes this paper.

II. Background

A. Cloud Trust Protocol (CTP)

The Cloud Trust Protocol (CTP) is a protocol which enables the cloud service consumers to request and retrieve trust related information from the cloud service provider [6], [7]. The information received is concerning the main attributes used in the assessment of any service. These attributes are security, integrity, compliance, privacy, and operational security history of service elements. CTP enables the cloud users to ask and get answers about the configuration and all the other specifications shown in [15]. This helps the user to do the assessment for the cloud service provider and regain the control in his/her hand [15].

The main purpose of CTP is to generate an evidence that everything is running based on the SLA agreement between the cloud user and the provider. CTP introduces a Transparency-as-a-Service (TaaS) used to perform monitoring with evidence based assurance. These evidences are based on pieces of information called the elements of transparencies. They offer testimony regarding important security configuration functional-characteristics for all those systems which potentially integrated with computing cloud. It also used to determine which cloud is best suited in order to meeting their processing requirements [16].

The CTP describes how the cloud consumer asks about an element of transparency (EoT) and how to package the answer. This is done through request/response technique over 24 Elements of Transparency (EoT). The 24 EoT represent all the types of requests that the cloud user can ask from the cloud service provider. The first two EoT represents the initiation and the termination of any CTP session. The other 22 EoT are used for getting information about specification and control oriented. They can be classified by type to evidence requests, provider assertions, provider notifications, policy introduction, SCAP and extensions or by family to Configuration, Vulnerability, Anchoring, Audit Log, Service Management, Service Statistics, Provider Capability and service Claims, Alerts, Users and Permissions, Configurations, Anchoring, Quotas, Alerts and Client defined [16]. The CTP is designed as an adaptable protocol to be adjusted according to the digital trust requirements of the cloud consumers and the functional situations of the cloud provider.

The CTP data model represents security, compliance and data governance attributes that can be queried by CTP clients. It was represented by using 10 structures. These structures are customer, service view, asset, attribute, measurement, metric, trigger, log entry, result and objective [19]. These structures represent the services offered through services, characterize the elements of the cloud system (physical or ethereal) through asset, a set of security attributes measured by measurements and characterized through attribute while the standardization of measurements is described in metric and trigger and Log entries are used to describe request/response situations regarding some measurements required by the consumer [19]. The CTP API uses the RESTful API for performing the request/response queries through HTTP methods such as GET, PUT, POST and DELETE.

B. CAIQ Assessment

CTP provides a way for the user to request evidence or certificates from the cloud service provider regarding the operation of a specific service. This information gives the user a whole picture about what he should expect while running the service. The client after using the service may have a feeling or an evidence based on experimentation that the service was done correctly according to the description given by the provider or differ which violates SLA agreement between the cloud provider and the consumer. Based on this information we aim to give the cloud provider the ability to assess his own service (self-assessment) and to give the user the capability to assess the service again after using it (feedback assessment). The two assessments increase make the output trust values more reliable by describing not only the service specifications but also the real behavior of the service.

The Cloud Security Alliance (CSA) generated a spread sheet containing 140 yes/no questions known as the Consensus Assessments Initiative Questionnaire (CAIQ) which covers the main attributes –compliance, data governance, and ...etc.– and used in the assessment process [5]. The CAIQ covers 98 controls under its framework. Each control has one or more questions about various cloud providers' capabilities and competencies. It is adopted to offer cloud customers a means of querying the providers without compromising infrastructure security; the questionnaire will also help to reduce the cloud providers burden of answering myriad queries. It is intended to assist both the cloud customer and cloud auditor in evaluating a potential cloud provider [5], [17], [18].

Self-assessments vs assessments by the clients: There are two types of assessments. The first type is a self-assessment operation. This type enables the cloud service provider to assess its own service behaviour. This was done before in many papers using the normal CAIQ assessment questionnaire [3], [21]. The trust value calculated from this type reflects only the service provider view but not the client. This is one-way trust relation between the provider and the client which is not sufficient. Trust relation have to be also based on customer's feedback for their usage of the services offered by a cloud service provider. So, the second type of assessments is those done by the clients based on their experience. Until now the Cloud Security Alliance (CSA) didn't make a specific version of the CAIQ questions to the cloud consumers. However, the Smals ICT for society group generated a two cloud security assessment models that can be used by clients whether they are normal clients or experts [20]. The normal client assessment model was usually used to compare between the service specification the client needs with the specifications offered by all the service providers while the expert client assessment enables the cloud consumer to assess the security level of a cloud service offered by a Cloud Service Provider. This can be done by answering questions –not only MCQ– covering four main characteristics expected of the cloud service: Governance, Identity and Access Management (IAM), IT Security and Operational Security. In this papers, we are going to use the expert client assessment model and we are going to select the questions that can be answered by Yes or No.

C. Subjective Logic over Subjective Opinions

Subjective logic extends standard logic and takes into consideration the uncertainty and the belief ownership. It is suitable for considering models with uncertainty and incomplete knowledge which is essential for the assessment method we use. The advantage of using subjective logic is the ability to distinguish between certain and uncertain conclusions as the uncertainty is taken in consideration in their calculations. Subjective logic presents operations that work over the subjective opinions (binomial subjective opinions in our case) such as addition, subtraction, complement, multiplication, comultiplication [22], [23]. For the purpose of this paper we are only interested in multiplication and consensus of opinions.

A binomial opinion over a variable x is represented in subjective logic by a quadruple of real numbers $\omega_x = (b_x, d_x, u_x, a_x)$ all from the interval [0…1], subject to the constraint $b_x + d_x + u_x = 1$. They are referred to as *belief*, *disbelief*, *uncertainty* and *relative atomicity* of x, respectively [22], [23]. Both the user and the provider opinions are expressed as binomial opinions. These binomial opinions are calculated based on the answers of multiple choices questionnaires designed specifically to assess the service from two different views (provider and user). We are going to use binomial operators such as product and consensus to calculate the overall provider and user opinion towards a specific service.

In section IV we define how opinions are calculated based on users' responses to questionnaires.

1) Multiplication of Opinions:

The multiplication (logic AND operator) between opinions ω_{x_1} and ω_{x_2} is denoted by $\omega_{(x_1 \wedge x_2)} = \left(b_{(x_1 \wedge x_2)}, d_{(x_1 \wedge x_2)}, u_{(x_1 \wedge x_2)}, a_{(x_1 \wedge x_2)}\right)$.

$$b_{(x_1 \wedge x_2)} = b_{x_1} b_{x_2} + \frac{(1 - a_{x_1}) a_{x_2} b_{x_1} u_{x_2} + a_{x_1} (1 - a_{x_2}) u_{x_1} b_{x_2}}{1 - a_{x_1} a_{x_2}}$$

$$d_{(x_1 \wedge x_2)} = d_{x_1} + d_{x_2} - d_{x_1} d_{x_2}$$

$$u_{(x_1 \wedge x_2)} = u_{x_1} u_{x_2} + \frac{(1 - a_{x_2}) b_{x_1} u_{x_2} + (1 - a_{x_1}) u_{x_1} b_{x_2}}{1 - a_{x_1} a_{x_2}}$$

$$a_{(x_1 \wedge x_2)} = a_{x_1} a_{x_2}$$

With a projected probability of $P_{(x_1 \wedge x_2)} = P_{x_1} P_{x_2}$[22], [23].

2) Consensus opinion of two opinions:

Given two opinions the consensus opinion is meant to reflect both opinions in fair and equal way. Assume the agents A and B have opinions $\omega_x^A = (b_x^A, d_x^A, u_x^A, a_x^A)$ and $\omega_x^B = (b_x^B, d_x^B, u_x^B, a_x^B)$ about a common variable x , respectively. The consensus opinion denoted by $\omega_x^{A,B} = \omega_x^A \oplus \omega_x^B = (b_x^{A,B}, d_x^{A,B}, u_x^{A,B}, a_x^{A,B})$ is defined by

$$b_x^{A,B} = \frac{b_x^A u_x^B + b_x^B u_x^A}{\mathscr{k}}$$

$$d_x^{A,B} = \frac{d_x^A u_x^B + d_x^B u_x^A}{\mathscr{k}}$$

$$u_x^{A,B} = \frac{u_x^A u_x^B}{\mathscr{k}}$$

$$a_x^{A,B} = \frac{a_x^B u_x^A + a_x^A u_x^B - (a_x^A + a_x^B) u_x^A u_x^B}{u_x^A + u_x^B - 2 u_x^A u_x^B}$$

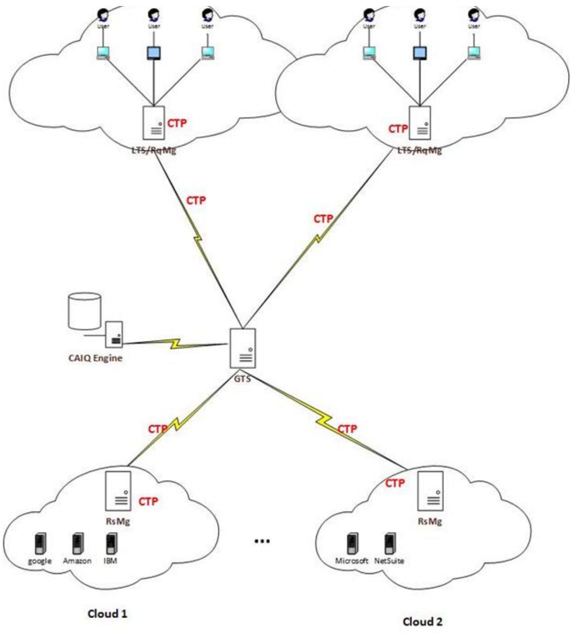
Where $\mathscr{k} = u_x^A + u_x^B - u_x^A u_x^B$, and this operator can't be applied on vacuous $(u_x = 1)$ or dogmatic $(u_x = 0)$ opinions. It is conditioned to be applied for uncertain opinions $(0 < u_x < 1)$ only [27].

III. Proposed System Architecture

Fig. 1 shows the infrastructure for the proposed trust management system. Any user might be a member of an organization, a group of users. For every group of users there exist a local trust server (**LTS/RqMg**). The **LTS/RqMg** is used as a local trust server while calculating the trustworthiness for a specific provider and as a request manager in the case of applying the CTP protocol. For every cloud, a receiving manager (**RsMg**) is used to respond to the request sent by the **RqMg** in the CTP protocol. A general trust server (**GTS**) is used to collect and store the overall trust values for the service providers in assessment operations and to just route the requests/responses in the CTP protocol. In the assessment operation, a CAIQ engine is used to store the CAIQ questioners and the assessed questioners from the users.

The system is designed to use the CTP protocol in order to get trust information about any service provider and based on this information an assessment could be done in order to get the digital trust for this provider. So, the system is working in 3 modes: CTP protocol, CAIQ assessment, and trust retrieving requests which asks the LTS and the GTS to give the user a list of all the providers offering a specific service based on their trust values. As shown in Fig. 1, Users can be fitted into two different group structures. A single separate user can build his own group and uses the GTS directly and as the group now consists of only one user, LTS doesn't add any additional feature to that 1-user group. For multi-users group, a Local Trust Server (LTS) is used for trust referencing while only one general Trust Server (TS) is used for the cloud. The LTS is used only within its group of customers. It is used to answer client trust requests locally depending on the assessments from the other clients inside the organization which are stored inside LTS. If the data stored in the LTS is not sufficient to answer a trust request from the customer -the client request trust information about new service or unassessed service– or it is out of date, the general TS is used as a reference to the LTS. The GTS also is used directly to answer trust requests from the normal separate users, that are not inside any organization. The GTS acts as an accumulator for all LTSs trust data.

Figure 1: Proposed system infrastructure.



Local Trust Server (LTS): The LTS contains trust data about what already assessed by any member of its group. It is initially empty. Once a customer assesses a specific provider, an entry will be added containing trust knowledge about this specific provider service and a copy of the calculated trust knowledge will be sent to the general trust server GTS. The trust data inside the LTS is organized in the following form shown in Table I.

Table I: Trust data inside a LTS.

Domain URL (name)	Service Type	Trust Value	Boolean Trust	Decision Time
…	…	…	…	…

Table II: Services' thresholds.3

Service Type	Threshold Trust Value
…	…

The trust value entry contains the trustworthy value calculated from each requested service, shown in Service Type entry, from a specific provider, shown in Domain URL entry, using Propositional Logic Terms PLTs. [3], [22], [23] Based on the threshold trust values stored in table II for each service type, a true/false trust value is calculated and stored in Boolean Trust entry. The decision time will be recorded in order to use it in updating the table.

General Trust Server (GTS): The general Trust Server TS contains all the trust data gathered from all LTS servers and the separated single users' assessments. The CTP protocol needs 24 bits to identify 24 elements of transparency EoT. Also, the provider domain name and the required service name (code) are needed also. So, the request can be designed shown in table III.

Table III: Request format.

00 CTP 01 CAIQ 1d Query	Domain Name	Service (Code)	24 bits to express 24 EoT items. The element required its bit is settled to 1.

Importance of LTS with GTS: Let's consider the case that we have two providers X and Y offer the same service and both are trustworthy. Assume also due to the bad distribution of provider X servers there is a place L where the service is not worked correctly. However, providers X and Y are offering a good service, place L users doesn't find it is not a good decision to ask X for the service and it is better to ask Y. This problem may appear also because of the incompatibility of the organization's hardware network structure with a specific provider demands. Because of that, LTS is very important in the case of assessment based on the typology. It contains a list of all the cloud service providers that offer services already used, assessed and verified to be trusted from users share the same organization. That overcomes the problem that the physical infrastructure between the cloud service provider servers and the client didn't count in the assessment operation. The details of different requests/responses that can be provided over the proposed system are shown below:

- CTP request/response:
  - The user asks for information relating to CTP. A CTP initiation request is sent with 00 leftmost flag. Once the initiation request is approved, CTP EoT can be requested also with 00 leftmost flags.
  - The LTS/RqMg now is working as a RqMg. The EoT bits are asserted according to the requests required.
  - The request is sent to the GTS which acts now as a router. It tells the request where should it go.
  - Once the CTP is received at a cloud, the RsMg is responsible for the response also with 00 leftmost flag.
  - The response is sent back from the RsMg to the RqMg via the GTS and then is delivered to the user.
- CAIQ Assessment request/response:
  - For those users who already used the CTP protocol to get trust information about a specific service provider, it is allowed to assess them.
  - An assessment request is sent with 01 leftmost flag from the user to the LTS/RqMg which now works as a LTS.
  - The request is forwarded from the LTS to the GTS which asks the CAIQ engine for the CAIQ questionnaire.
  - The CAIQ questionnaire is sent back to the user via GTS and LTS servers.
  - Once the user has finished the assessment, the trust value is calculated and stored at the LTS and a copy of it also will be sent to the GTS. So, now LTS contains entries for all the providers assessed from a member of the same organization with their trust values generated only from it while GTS contains entries for all the providers assessed from all organizations with the updated trust values.
- Trust query request/response:
  - The cloud consumer can ask for a list of all the providers offer a specific service. This is a request with 1d leftmost flag. This request has one of two destinations, either LTS or GTS.
  - The LTS send a response directly if there exist at least an entry in his table with an accepted Boolean trust (true) and not timed out for the provider offer this service.
  - If LTS has no direct answer or is not Boolean trusted or there was an entry but timed out, the request will be forwarded to the GTS which answers it.
  - Every amount of time, all the entries exist in the LTS's table which are timed out have to be updated from the GTS throw updating request.

IV. Proposed Assessment Technique

We suggest to use assessments based on Yes, No and Unknown answers. There are two types of assessments. (i) The provider self-assessment. (ii) The cloud consumer assessment. we will use the provider self-assessment technique shown in [3] to generate the initial trust value. In this paper, we provide a consumer assessment to evaluate the service offered by a provider. A Yes/No questionnaire is used to get an overall idea about the consumer experience while using the service. The consumer questionnaire answers are represented by a binomial subjective opinion. This binomial opinion is visualised inside Barycentric Coordinates in order to classify it into one of rating classes which is used to find the aging factor which is responsible for updating the initial trust value.

Figure 2: A binomial opinion representation inside Barycentric coordinates.

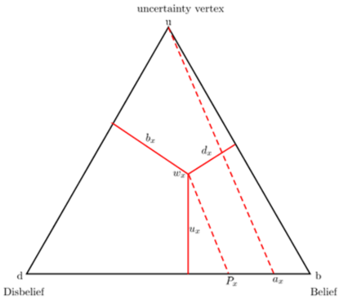
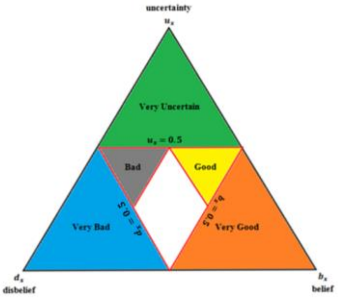


Figure 3: A binomial opinion rating classification.



A. *Barycentric Coordinates and Opinion Visualization*

The Binomial subjective opinions $\omega_x = (b_x, d_x, a_x, u_x)$ can be visualized using the Barycentric coordinates inside a triangle with uncertainty, belief and disbelief vertices as shown in Fig. 2. The triangle used here is equal sides. The opinion is represented as a center of gravity (barycenter or geometric centroid) of locating three masses M_A, M_B and M_C at the triangle vertices. These masses are located over three axis perpendicular over the opposite triangle side of each vertex. These masses are represented b_x, d_x and u_x respectively. The base rate a_x is represented by a point in the base. The line connecting the u vertex to the point represented by a_x is called the director. The projected probability P_x of an opinion ω_x can be determined by drawing a line from the opinion point ω_x to the base and parallel to the director line.

For homogenous Barycentric coordinates, the edges are normalized in order to achieve $b_x + d_x + u_x = 1$. The projected probability can be calculated as follow, $P_x = b_x + u_x a_x$.

Opinions can be visualized more in details by applying the fuzzy concepts in the Barycentric coordinates in order to get a classification for every opinion. In our model, we have 6 rating classes for the opinion represented inside the triangle as shown in Fig 3. These classes are: very good, good, very bad, bad, unnamed, and very uncertain classes. This classification is based on the values of the belief b_x, disbelief d_x, and uncertainty d_x. Table IV shows the ranges of these three variables inside each region.

Table IV

Region	**Belief**	**Disbelief**	**Uncertainty**
Very Good Certain	$b_x \geq 0.5$	$d_x < 0.5$	$u_x < 0.5$
Good Certain	$0.25 < b_x < 0.5$	$d_x < 0.25$	$u_x < 0.5$
Very Bad Certain	$b_x < 0.5$	$d_x \geq 0.5$	$u_x < 0.5$
Bad Certain	$b_x < 0.25$	$0.25 < d_x < 0.5$	$u_x < 0.5$
Unnamed Certain	$0.25 \leq b_x < 0.5$	$0.25 \leq d_x < 0.5$	$u_x < 0.5$
Very Uncertain	---	---	$u_x \geq 0.5$

Collecting Opinions, Aggregation, and Aging

Providers have the ability to assess their services themselves. This produces an initial trustworthiness value for every provider service. In this paper, we are giving the user the power to reassess that service based on his experience dealing with it. Consumers' opinions should be collected somehow and propose a technique of how these opinions are going to changes the initial assessment (aggregation and aging).

Aggregation of new and old opinions

An agent is allowed to rate any service by simply answering the MCQ questionnaire provider for consumers. From the agent's answers we can calculate his opinion $\omega_x = (b_x, d_x, u_x, a_x)$ via subjective logic (AND and Consensus). This opinion will be visualized via Barycentric coordinates. The opinion is going to be classified into one of six predefined different rating levels based on its location inside the Barycentric triangle. The reputation score is going to be changed by an aging factor which is different from each rating class to other.

The simplest way to do the aggregation of ratings is by using the simple addition. This can be done by using an aggregation constant $\lambda \in [0,1]$. The value of λ is the factor that control the rapidity whether by increasing or decreasing it as a function of time. The aggregation has no effect on the original ratings if $\lambda = 0$ and completely forgotten after a single time period while it has the largest effect with $\lambda = 1$.

Let's define

- $r_{y,t}$ is the initial rating value (only provider) generated from the provider self-assessment for service y.
- $R^x_{y,t}$ is the old rating value (provider and user x) over time t for service y.
- $R^x_{y,(t+1)}$ represents the overall (provider and user x) new accumulated rating value after time period $t + 1$ for service y.

- $R_{y,(t+1)}$ represents the overall (provider and all users) new accumulated rating value after time period $t+1$ for service y.

In order to give a permission to any user to do the assessment any number of time, our method of calculating the reputation (rating) value generated from any agent x towards service y depends not only on the current opinion outcome factor k_{t+1} but also on the previous one k_t. The idea behind doing another assessment is to remeasure the reputation again and produce new value instead of the generated old one. so, our method based on updating the overall reputation value with the new opinion and removing the old one for all the users that do many assessments.

Assuming that the value of previous opinion outcome factor for those agents that do their first assessment is $k_t = 0$. The new accumulated rating $R_{y,(t+1)}$after time period $t+1$ can be expressed as:

- For the first user assessment: $R^x_{y,(t+1)} = \lambda' + r_{y,t}$ where $0 \leq \lambda' \leq 1, \lambda' = (k_{t+1} - k_t)\lambda$.
- For any user assessment except the first one: : $R^x_{y,(t+1)} = \lambda' + R^x_{y,t}$ where $0 \leq \lambda' \leq 1, \lambda' = (k_{t+1} - k_t)\lambda$.

The overall reputation (rating) generated from all users $x \in X$ -where X is the set of all users did the assessments- is simply generated from the average overall users' ratings as follows:

$$R_{y,(t+1)} = \frac{\sum_{x \in X} R^x_{y,(t+1)}}{|X|}$$

The previous way of collection users' opinions depends only on the last assessment of each user by removing all the history created before. Another way of collecting users' opinions is to do the aggregation between the last assessment outcome for each user with an aged value of the history generated by the same user. Let's define an aging factor $\Lambda \in [0 \ldots 1]$. The value of Λ determines the history ratio of the user's opinions that contributes with the new opinion to generate the current reputation value of the user towards any service. The history is forgotten as shown in the previous method if $\Lambda = 0$ and contributes with the full ration if $\Lambda = 1$. [25]

The new accumulated rating $R_{y,(t+1)}$ after time period $t+1$ can be expressed as:

- For the first user assessment, there is no assessment history for the user x towards the service y. So, there is no need for doing any form of aging here in the first user assessment: $R^x_{y,(t+1)} = k_{t+1}\lambda + r_{y,t}$ where $0 \leq \lambda \leq 1$.
- For any user assessment except the first one: $R^x_{y,(t+1)} = k_{t+1} \times \lambda + \Lambda \times R^x_{y,t}$ where $0 \leq \lambda \leq 1$.
  - For decreasing the effect of the history we use $\Lambda = 0.01$.
  - For increasing the contribution of the history in the calculation of the current reputation value we use $\Lambda = 0.99$.

The average rating $\mathbb{R}^x_{y,(t+1)}$ generated by user x towards the service y at the current time $t+1$ is calculated as follows:

$$\mathbb{R}^x_{y,(t+1)} = (R^x_{y,(t+1)})/(\mathbb{N})$$

Where $\mathbb{N}$ is the number of assessments for the user x towards the service y.

The overall reputation (rating) generated from all the users $x \in X$ were X is the set of all users did the assessments is generated from averaging all the users; average ratings as follows:

$$\mathbb{R}_{y,(t+1)} = \frac{\sum_{x \in X} \mathbb{R}^x_{y,(t+1)}}{|X|}$$

The value of k is determined as follow and depends on the rating class for the consumer opinion:

- For very good and certain class ($k = 1$).
- For good and certain class ($k = \frac{1}{2}$).
- For very bad and certain class ($k = -1$).
- For bad and certain class class ($k = -\frac{1}{2}$).
- For un-named and certain class ($k = \frac{1}{4}$ if $P_x \geq 0.5$ and $k = -\frac{1}{4}$ if $P_x < 0.5$)
- For very uncertain class ($k = 0$).

Overall description for the assessment technique

Provider Side: We will use the same CAIQ assessment used before from the providers to assess their own services and create their own initial trust value.[3]

Consumer Side: This is our contribution of giving the consumer the ability to reassess the services and modify the initial trust values generated by the providers based on the clients' experience with the service offered. The clients have their own version of questionnaire which is similar to the providers CAIQ but from the client point of view. This questionnaire gives the overall opinion of the user to a specific service. The questionnaire is based on four attributes Governance, Identify and Access Management, IT Security and Operational Security. Each attribute has a number of sub-attributes. The overall client opinion can be calculated from the questionnaire as follows:

1. For each sub attribute calculate $\omega_{sub} = (b_{x,sub}, d_{x,sub}, u_{x,sub}, a_{x,sub})$ based on the Yes/No answers including the of the not applicable.

$$b_{x,sub} = \frac{p}{p+n+m}$$
$$d_{x,sub} = \frac{n}{p+n+m}$$
$$u_{x,sub} = \frac{m}{p+n+m}$$
$$a_{x,sub} = \frac{1}{2}$$

Where p is the number of Yes answers, n is the number of No answers and m is the number of the unknown answers [28].

2. For each attribute, calculate the product of all the opinions generated for all the sub attributes inside that attribute $\omega_{att} = \prod(\omega_{sub})$.
3. For sub-opinions with some uncertainty, the overall opinion will be collected by the consensus operator assuming that all the four attributes assess the service from different point of view $\omega_x = \omega_x^{att1} \oplus \omega_x^{att2} \oplus \omega_x^{att3} \oplus \omega_x^{att4}$.

4. For sub-opinions with 0 or 1 uncertainty, the overall opinion will be generated by simple product operator between them.
5. The user's opinion is going to be visualized using Barycentric coordinates in order to know the aging factor k of the user's opinion on the initial trust value generated by the provider.
6. Do the aggregation where λ is the aggregation value Fixed.

V. Conclusion

We can conclude that the suggested network infrastructure gives the user the ability to request CTP information, do assessments via questionnaires and query the general trust server to get a snapshot of old trust information for a specific provider. Moreover, to have reliable trust, not only the providers should do the services assessments but also the users. For the user's multiple assessment, it is sufficient to keep the latest rating extracted from his opinion without aging. The ongoing work is to do tests over the suggested assessment technique, in particular using barycentric coordinates for visualization. This paper assumes that every user is a trusted user which means that his opinion affects the trust without any revision. The future work is to detect and remove the untrusted users (malicious users) before doing the assessment.

References

[1] F. Doelitzscher, C. Reich, M. Knahl, A. Passfall, and N. Clarke, "An agent based business aware incident detection system for cloud environments," Journal of Cloud Computing: Advances, Systems and Applications 2012.

[2] A. Sumetanupap and T. Senivongse, "Enhancing Service Selection with a Provider Trustworthiness Model", Eighth International Joint Conference on Computer Science and Software Engineering (JCSSE), 20ll, P(281-286).

[3] S. Habib, S. Ries, M. Muhlhauser and P. Varikkattu, "Towards a Trust Management System for Cloud Computing Marketplaces: using CAIQ as a trust information source", Security and Communication Networks, 2014.

[4] Jøsang A, Ismail R, Boyd C, "A survey of trust and reputation systems for online service provision", Decision Support Systems 2007, 43(2),P(618 – 644).

[5] CSA. "Consensus assessments initiative" https://cloudsecurityalliance.org/research/initiatives/consensus-assessments-initiative/

[6] Knode, Ronald, "Digital Trust in the Cloud" August 2009. www.csc.com/security/insights/32270-digital_trust_in_the_cloud

[7] Knode, Ronald with Egan, Douglas, "Digital Trust in the Cloud: Into the Cloud with CTP – A Precis for the CloudTrust Protocol, V2.0" ,July 2010, http://www.csc.com/cloud/insights/57785-into_the_cloud_with_ctp

[8] Lukan, D., "CloudTech. Retrieved from The top cloud computing threats and vulnerabilities in an enterprise environment" (2014, November 21). http://www.cloudcomputing-news.net/news/2014/nov/21/top-cloud-computing-threats-and-vulnerabilities-enterprise-environment/

[9] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger and D. Leaf. "NIST Cloud Computing Reference Architectures: Recommendations of the National Institute of Standards and Technology", Cloud Computing Program Information Technology Laboratory, National Institute of Standards and Technology.Gaithersburg,2011. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

[10] Blomqvist K., "The many faces of trust", Scand J Manage 13(3): P(271-286), 1997.

[11] Mayer R, Davis J, Schoorman F, "An integrative model of organizational trust: Past, present, and future" Acad Manage Rev 20(3): P(709–734), 1995.

[12] "Merriam-Webster's Collegiate Dictionary" 11^{th} Edition, 2015 by Merriam-Webster, Inc. http://www.Merriam-Webster.com

[13] Huang J, Nicol D, "A formal-semantics-based calculus of trust" Internet Comput IEEE 14(5): P(38–46), 2010.

[14] L. Wu and R. Buyya, "Service level agreement (SLA) in utility computing systems" CoRR, 2010.

[15] Knode, R. and Egan, D.,"Digital trust in the cloud: A précis for the cloudtrust protocol (v2.0)} ,P(1–40), 2010. http://assets1.csc.com/cloud/downloads/wp_cloudtrustprotocolprecis_073010.pdf

[16] Shou-Xin Wang, Li Zhang, Shuai Wang, and Xiang Qiu, "A cloud-based trust model for evaluating quality of web services", Journal of Computer Science and Technology, vol. 25, no. 6, P(1130-1142), 2010.

[17] D. Catteddu and G. Hogben,"Cloud Computing: benefits, risks and recommendations for information security", Technical Report. Heraklion: European Network and Information Security Agency, 2009.

[18] CSA, "Security guidance for critical areas of focus in cloud computing v3.0", Technical Report, Cloud Security Alliance 2009.

[19] "CTP Data Model and API, rev.2.13", Cloud Security Alliance, October 2015 https://downloads.cloudsecurityalliance.org/assets/research/cloudtrust-protocol/CTP-Data-Model-And-API.pdf

[20] T. Martin, "Modèle d'évaluation de sécurité cloud", Smals Research. https://www.smalsresearch.be/tools/cloud-security-model-fr/

[21] N. Bhensook and T. Senivongse, "An Assessment of Security Requirements Compliance of Cloud Providers", IEEE 4th International Conference on Cloud Computing Technology and Science, P(520--525), 2012.

[22] A. Jøsang and D. McAnally, "Multiplication and comultiplication of beliefs", International Journal of Approximate Reasoning 38 : P(19–-51), 2005.

[23] A. Jøsang, "Book : Subjective Logic", Universitas Osloensis, 2015

[24] W. Li and L. Ping, "Trust Model to Enhance Security and Interoperability of Cloud Environment", Lecture Notes in Computer Science, vol. 5931, P(69--79), 2009.

[25] A. Jøsang, X. Luo and X. Chen, "Continuous Ratings in Discrete Bayesian Reputation Systems", The International Federation for Information Processing, vol. (263), P(151--166), 2008.

[26] A. Whitby, A. Jøsang and J. Indulska, "Filtering Out Unfair Ratings in Bayesian Reputation Systems", Autonomous Agents and Multi Agent Systems Conference, 2004

[27] A. Jøsang, "TRUST-BASED DECISION MAKING FOR ELECTRONIC TRANSACTIONS" Proceedings of the Fourth Nordic Workshop on Secure Computer Systems (NORDSEC'99), Stockholm University, Sweden, 1999

[28] D. Ceolin, A. Nottamkandath, and W. Fokkink, "Subjective Logic Extensions for the Semantic Web"