Ethical Trust in Cloud Computing Using Fuzzy Logic

Ankita Sharma[1(✉)] and Hema Banati[2]

[1] Jagannath University, Jaipur, Rajasthan, India
Ankita.sharma@jimsindia.org
[2] Department of Computer Science, University of Delhi, New Delhi, India
banatihema@hotmail.com

Abstract. Cloud computing, today, has gained wide acceptance by business enterprises across the globe. With growing popularity of cloud computing and a considerable amount of research already conducted on the fundamental issue of trust in the cloud, researchers are now focused on determining the linkage between ethics and trust. Ethical issues in cloud depend on the particular application and current circumstances. The paper proposes a novel technique of computing ethical trust placed on a service provider. The approach takes into consideration various factors which affect trust and ethics; as qualitative inputs through a customized interface. The accepted inputs are fuzzified and using a special set of designed rules, an ethical trust value is computed. The resultant output is subsequently de-fuzzified using the centroid method The calculated degree of ethical trust can help in ascertaining the significance of a service provider and is therefore of great utility in the area of cloud computing.

Keywords: Cloud · Ethics · Trust · Fuzzy systems

1 Introduction

In today's dynamic and competitive business world, cloud computing has proved to be a boon to commercial enterprises. Cloud computing includes a set of resources that are allocated as a when on demand. Cloud computing is a collection of various resources which provided to the customer via the internet. Cloud computing has made it possible for the users to get in use of all the virtual resources with the help of internet. An example of cloud services is Google Engine, Oracle Cloud, Office 365. But nowadays as cloud computing is growing it is leading to severe security issues and because of this, the trust factor comes into picture [14]. Cloud computing comprises of three layers i.e. Infrastructure, Platform, and Application. IAAS means Infrastructure as a service; PAAS means Platform as a service; SAAS means Software as a service The SaaS layer in the cloud helps the customer to run an application of their choices such as Inventory Management and Customer Relations Management. Software as a Service (SaaS) also expels the need to install the software on the system and provides the advantage to run the software as an application on the customer's own computer which in turn simplifies the maintenance and support of the software on the customer's end. PaaS stands for Platform as a Service. To make use of this service an organization must have a good

J. Wan et al. (Eds.): CloudComp 2016, SPNCE 2016, LNICST 197, pp. 44–55, 2018.
https://doi.org/10.1007/978-3-319-69605-8_5

number of computing experts. This service is popular amongst the developers who need to test their services in multiple platforms such as various versions of Windows, Mac, Linux operating systems. IaaS stands for Infrastructure as a Service. This service is most suitable for large businesses only as the customer is expected to manage both the hardware and the software that run on this hardware. So instead of purchasing the servers, software's, data space the client's buys the resources as a complete outsourced service.

It saves the cost of carrying out business, but, of late cloud computing domain is flooded with issues of ethics and trust. Trust is defined as a generation of a feeling of assurance or confidence, of one party onto another party who are somewhat bounded by certain terms and conditions. It is this element of *bounded* which ensures the process of building trust between two parties. An example of trust for a cloud vendor includes sending a trusted employee to the customer's site with the assurance that *this* trusted employee will be able to handle the technical problems reported by the customer. Here, the trust is implied in the *technical domain* of the *said* employee. The trust factor is based on evidence and subjective logics and is further used for the evaluation of security issues based on historical data. [12] A practice, which is specially drafted by business units to ensure that the trust is adequately implied is ethics and is this implication has aptly demonstrated the principles of ethics. For example, ethics for a cloud computing vendor includes an organization-wide *policy*, and *practice* of the policy of never divulging the details of *confidential data* of a client to another third party, except, as specified by the policy in its exceptions clause. For example, an exception could be to provide details to government authorities or tax authorities.

Evaluating Trust for a cloud computing service is a complex task as it is a qualitative concept. The current research work aims to address the issue of trust on cloud computing and also to provide an effective mechanism to evaluate services of cloud provider based on trust and ethics. For a reliable cloud provider, a mechanism needs to be devised which effectively ensures clients that service provider is trustworthy and its services will be efficiently followed with ethics. There have been several models proposed for calculating trust e g. Trust Management Model for Cloud Computing Environment [15]. This model analyzes the properties of trust in a cloud environment. It follows the approach that the value of trust was evaluated based on the uncertainty of each by computing the decay function, number of positive interactions, reputation factor and satisfaction level for the collected information But the model does not address the issue of Ethics. In give name [17] the authors have explained security, privacy, accountability, audit ability as factors affecting user's trust in cloud computing but again have not accounted for ethics in the same. The service models of cloud computing are being introduced in [12] and the authors have talked about security as the main concern which acts as a hurdle from cloud computing being used widely. Without ethics trust becomes uncertain, because ethics provides integrity in a way of services provided, so the advantage of our model is that it is considering the factors which affect trust and ethics altogether, taking those factors into consideration ethical trust index is calculated. Higher the Value of this index, more the reliable is a service provider.

Worth mentioning is the fact that the issue of trust was already in vogue since the advent of cloud computing technology, on account of the fact of placing confidential

data to another party, but the question of ethics has slowly made its way in the cloud arena [8] Ethical trust is the implementation of a feeling of assurance or confidence between the client and server following some principles.

Also, further fuzzy set logic is developed that explains the human perception in a better manner. An approach is developed that devises the major aspects of trust and ethics relationship between cloud providers and users. All the dimensions of trust and ethics are represented with a fuzzy framework and degree of ethical trust is calculated [7].

This paper proposes a distinct method to calculate the ethical trust value in a cloud computing service provided by a vendor. The structure of the paper is as follows. Section 2 identifies the various factors that impact the calculation of ethical trust. Section 3 outlines the approach used for computing the ethical trust value followed by the prototype of the tool developed. Section 4 is based on the experimentation and results of the ethical trust index calculated summarizing up by the conclusion in Sect. 5.

2 Parameters for Calculating Ethical Trust

In this paper, we identify the parameters which can affect the ethical trust evaluation of IaaS.

2.1 Control

Cloud computing supports the outsourcing of data to third party service providers. All the information is locally stored in the cloud. Therefore the user places his computation and data on machines which are not directly under control. So a majority of users or customers claim their control over the data [2].

Also, the organizations suffer a huge loss of by providing direct control of data. The risks associated with cloud computing include the following unauthorized access to data, corruption of data, any kind of failure in the infrastructure [6]. So because of the above factors, there comes a contradiction between the outside data and in between the organization. This process is referred to as de-parameterization of data: “removal of a boundary between an organization and the outside world.” This further affects not only the border of the organization’s IT infrastructure, but also the organization’s accountability fades out eventually [6]. In a large organization, it becomes difficult to correct the consequences created by a single person.

2.2 Division of Responsibility

The responsibility of data is divided between the customer and the service provider and none of them is in a good position to represent them [2]. This eventually leads to a problem in ethical computing which is referred as “Division of Responsibility”. This division of work at times leads to many undesirable consequences and no one can be held responsible for the same. In cloud computing whenever a specific service delivered to a user depends on it depends on a large number of factors of the other system. Cloud computing typically makes use a service-oriented architecture (SOA) in which all the services are combined into large applications which are further provided to the

end users. Therefore this complex structure of cloud makes it difficult to determine who is responsible in case something undesirable happens. Hence the problem of many hands working together still persists.

2.3 Accountability

The data majorly the personal data that is to be stored in the cloud should be managed properly. It should be made sure that the users and the consumers both should be able to manage the data on the cloud. If a problem appears anytime, they should be able to determine which of them is responsible [2]. For the cloud user, the risk of privacy in cloud computing can be greatly reduced if the organizations providing cloud computing services combines the contractual terms and private policies to create an accountability in the form of transparent, enforceable commitments that are responsible data handling [1]. It should be taken care what all is being recorded and to who all the particular record is made available to.

There are few key elements which provide the provision of accountability within the cloud:

(1) Transparency
(2) Assurance
(3) User Trust
(4) Responsibility.

2.4 Privacy

Many of the companies providing cloud services store huge terabytes of data which might include personal information which is further stored in data centers in countries all around the world. Privacy becomes a major issue in this case [5]. All the privacy concerns are taken care by the governments, researchers, users, and providers of cloud services. Moreover majorly whenever there is a discussion about the ethical issue, cloud privacy is the main concern but on the other hand it is difficult to explicitly describe the concerns [3]. In general the basic aim to constrain the access to personal data which helps in prevention to acquire data and put a stop to the illegal use of information related to other persons [3]. So as the data is no more stored locally the control over the data now comes in the hands of the cloud service provider. The consumers of cloud have to completely trust the cloud provider that their data is safe and will not be leaked to the outside world. Also different service providers have different options in terms of privacy and the consumer will never be clear with which service provider they are dealing with. Both reasons imply that to consumers it will not always be clear what they can expect from service providers in the cloud concerning privacy [7].

The parameters outlined above do not have crisp values. They are qualitative in nature as they are based on the subjectivity of the user opinion. Specifying a numeric quantity for a subjective concept is difficult and introduces a degree of imprecision, or uncertainty. To handle this, this contribution employs fuzzy logic. It proposes a distinct method of ethical trust calculation keeping in consideration the subjective nature of the various influencing factors, explained above.

3 Evaluating Ethical Trust with Fuzzy Interface

This section presents an algorithm which takes into consideration the factors affecting trust on cloud (listed above) as inputs. Since these inputs are qualitative in nature, hence they are appropriately transformed into numerical values by applying triangular member functions and subsequently defuzzified through the centroid method.

Figure 1 presents the various stages of the fuzzy logic applied for trust index evaluation.

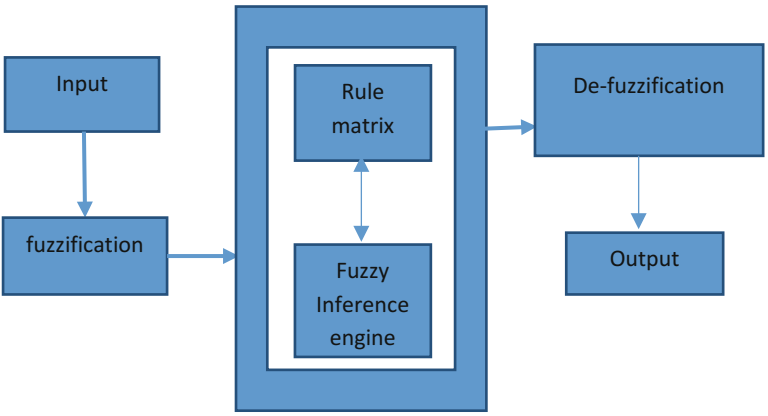


Fig. 1. Fuzzy logic controls analysis flow.

The initial qualitative input is accepted from the user, where the user specifies the required degree of the considered parameters viz. the control, division of responsibility, accountability and privacy in the service being considered. These values are then fuzzified by using membership functions for predefined input in this paper utilizes the triangular member function for the same.

A triangular MF is defined by three input parameters {a, b, c} as follows:

$$\text{triangle}(x; a, b, c) = \begin{cases} 0, & x \le a. \\ \frac{x-a}{b-a}, & a \le x \le b. \\ \frac{c-x}{c-b}, & b \le x \le c. \\ 0, & c \le x. \end{cases}$$

By using min and max, we can have an alternative expression for the preceding equation:

$$\text{triangle}(x; a, b, c) = \max\left(\min\left(\frac{x-a}{b-a}, \frac{c-x}{c-b}\right), 0\right)$$

Our chosen input parameters can have range of values between low, medium and high, Fig. 2 is depicting fuzzified of input values using triangular input function.

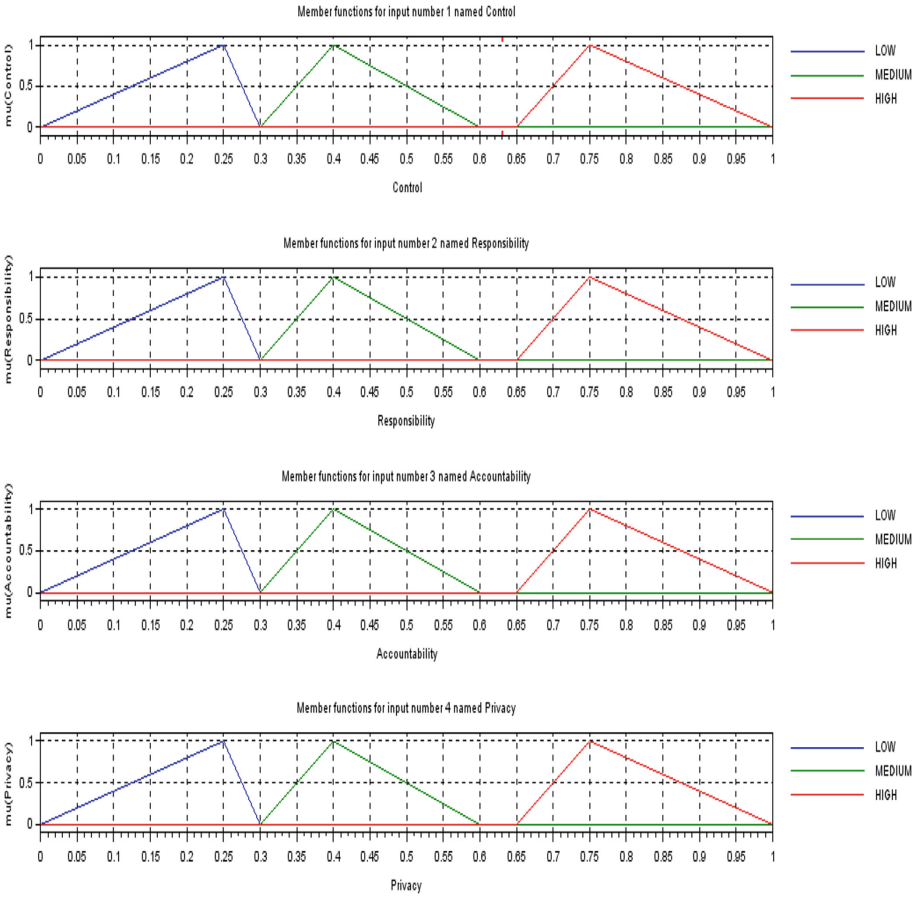


Fig. 2. Fuzzification of inputs using triangle function

The fuzzified input is then processed through the rule matrix (Table 1) which comprises of specifically designed rules. These are as follows:

1. If Control is LOW and Responsibility is LOW and Accountability is LOW and Privacy is LOW then TrustEthicsIndex is LOW.
2. If Control is LOW and Responsibility is MEDIUM and Accountability is MEDIUM and Privacy is LOW then TrustEthicsIndex is LOW.
3. If Control is MEDIUM and Responsibility is MEDIUM and Accountability is LOW and Privacy is HIGH then TrustEthicsIndex is MEDIUM.
4. If Control is MEDIUM and Responsibility is MEDIUM and Accountability is MEDIUM and Privacy is MEDIUM then TrustEthicsIndex is MEDIUM.
5. If Control is HIGH and Responsibility is HIGH and Accountability is HIGH and Privacy is HIGH then TrustEthicsIndex is HIGH.

Table 1. Samples of fuzzy rules for ethical trust evaluation of IaaS

Control	Division of responsibility	Accountability	Privacy	Degree of ethical trust
Low	Low	Low	Low	Low
Medium	Low	Low	Medium	Low
Medium	Medium	Low	High	Medium
Low	Medium	Medium	Low	Low
Medium	Low	Low	High	Medium
Medium	Medium	Medium	Medium	Medium
High	High	Low	High	Medium
Low	High	High	Low	Medium
High	Low	High	High	Medium
High	Medium	Medium	High	Medium
Medium	High	Medium	Medium	Medium
High	High	High	High	High

The final output is subsequently de-fuzzifed using centroid method to find a single crisp value which defines the output of a fuzzy set. Centroid Method is the most widely used methods amongst all the defuzzification methods [19, 20]. This method provides a center of the area under the curve of the membership function. For complex membership functions, it puts high demands on computation. It can be expressed by the following formula

$$z_0 = \frac{\int \mu_i(x) x dx}{\int \mu_i(x) dx}$$

where z_0 is de-fuzzified output, u_i is a membership function and x is output variable.

This final value provides the degree of the ethical trust of a single user in the respective service. However the trust index of a user is not based on a one time computation of trust degree. It needs to take in account the experience of the user in the relevant field and the level of expertise of the user. Thus the trust index for a single user is computed as below

$$\textbf{Ethical trust Index}\,(\mathbf{T}) = (\boldsymbol{U} \times \boldsymbol{E}) + \boldsymbol{O}$$

where U is Degree of Ethical trust calculated above using fuzzy logic.

And E is the experience of a user and significance of this factor, higher level of experience a user has more will be the values assigned, more experience also means User is more familiar with usage of cloud computing services. Experience of user can have following sample values in Table 2 below:

Table 2. Sample values of experience factor for ethical trust evaluation of IaaS

Experience of user	Value assigned
>1	0.1
1–3 years	0.5
3–8 years	0.75
8–10 years above	1.0

Table 3. Sample values of ownership factor for ethical trust evaluation of IaaS

Ownership of user	Value assigned
Trainee/non-IT staff	0.1
Developers/testers	0.4
Manager level users	0.8
Admin user	1.0

O is the ownership level of the user. Ownership is related to the rights allocated to a user. Higher the authority higher the rights of a user. For example Admin User and Manager level User will have the highest rights, they will have most of the or all of the rights to access all the cloud services so eventually they can provide better feedback of services used. The only exception to this factor is their level of experience, if user is not experienced with usage of cloud services even though he has all the access then his experience factor will be having low value.

Ownership can have different values based on user access level. Table 3 is showing sample values of Ownership factor:

For n number of users in the system, ethical trust index can be calculated as follows:

$$\mathbf{T} = \frac{\sum (\boldsymbol{Un} \times \boldsymbol{En}) + \boldsymbol{On}}{\boldsymbol{n}} \quad (\text{For multiple users where is n } > 0)$$

The Ethical trust index is calculated and the normalized value of the ethical trust index will vary between 0 and 1 as depicted in Fig. 3.

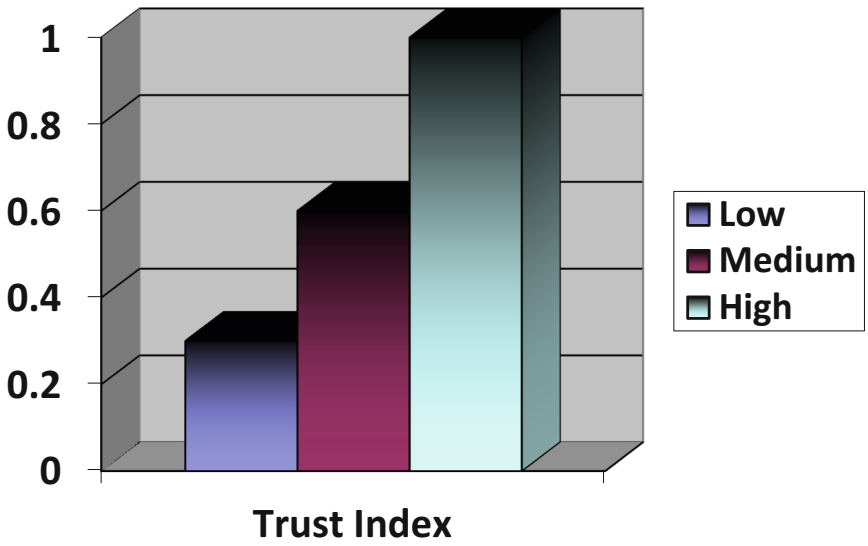


Fig. 3. Sample values of trust index

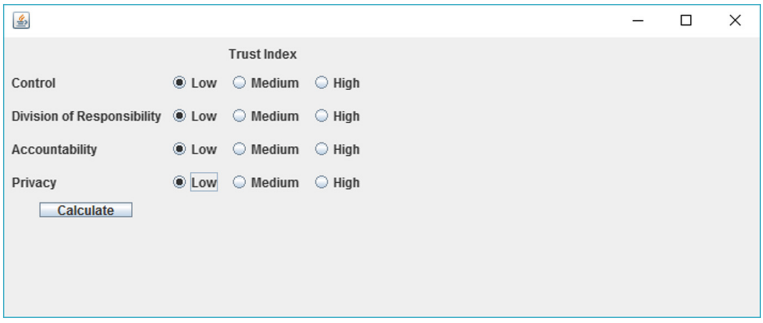
4 Experimentation and Results

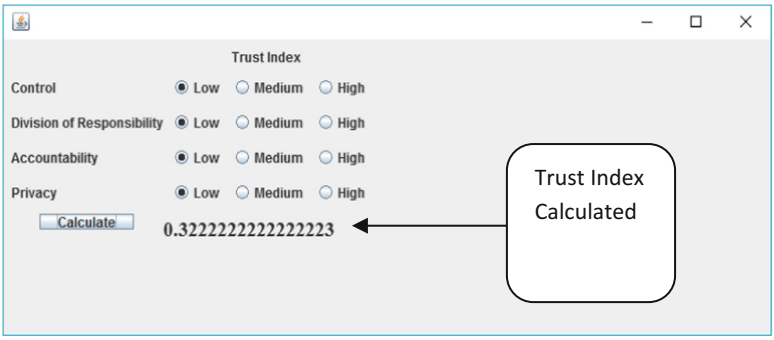
A prototype based on the above approach has been developed using 64 bit Java SE Development toolkit update 60 and also using jFuzzyLogic open source library on the following configuration of hardware:Intel i5 5th Gen processor 2.7 GHz CPU speed, with 8 GB of RAM and with 1 TB HDD. It accepts as input the parameters: Control, Division of responsibility, Accountability and Privacy in form of rating gathered for a cloud provider.

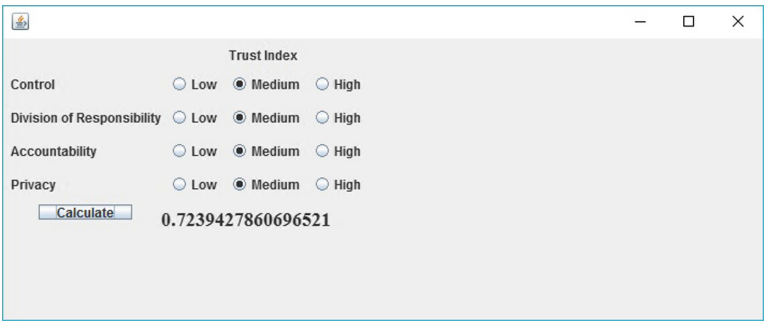
The interface developed is simplistic in nature as it prompts the user for each of parameter. Depending on the user requirement of each parameter a qualitative input is provided in the form of three values Low, Medium, and High. Limitation of possible three values for each parameter is kept to minimize possible fuzziness in user's inputs. All the calculations are backend through a set of rules and the user is simply provided on the click of Calculate button, a precise index of the ethical trust. The calculated value is not reflected back as a qualitative value, to ensure dynamism in the interpretation of the value. A value of 0.75 might be acceptable as "**high"** under certain conditions for some users rather than a value of 0.85. Thus the users are free to decide their own range of Low, medium and High ethical trust values.

The model can be extended with more parameters and a wider range of inputs to fine tune the output result. The significant issue is the generation of a quantitative value for a qualitative concept.

The screenshots below presents some sample screens of the designed interface.

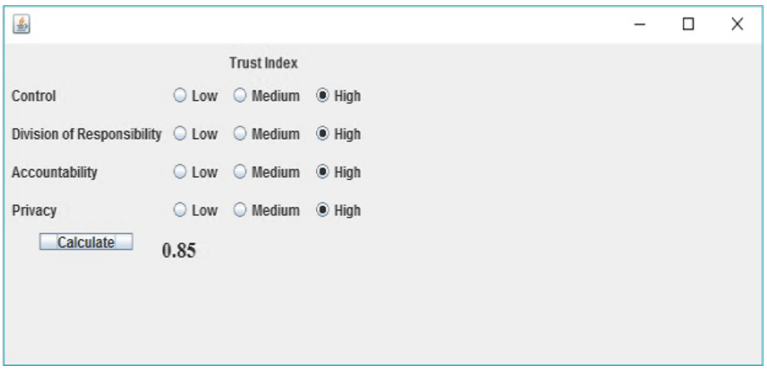





Trust Index
Control Low Medium High
Division of Responsibility Low Medium High
Accountability Low Medium High
Privacy Low Medium High
Calculate
0.7239427860696521


Trust Index
Control Low Medium High
Division of Responsibility Low Medium High
Accountability Low Medium High
Privacy Low Medium High
Calculate
0.32571585903083716


Trust Index
Control Low Medium High
Division of Responsibility Low Medium High
Accountability Low Medium High
Privacy Low Medium High
Calculate
0.7184210526315792


Trust Index
Control Low Medium High
Division of Responsibility Low Medium High
Accountability Low Medium High
Privacy Low Medium High
Calculate
0.85

This application takes all these inputs as a fuzzy set and de-fuzzify them using centroid algorithm [13] and based upon the rules in Table 2 it calculates the Trust Index. The prototype above assumes a Trust index between value 0 to 0.40 is low and from 0.50 to 0.75 is medium and in between 0.75 to 1.0 is high. More high the trust index more reliable the services are.

5 Conclusion

This paper proposes a distinct approach to compute a quantitative value of f ethical trust for cloud computing services. The approach recognizes the fuzzy nature of the significant factors which affect the trust on cloud providers and computes a distinct degree of ethical trust pertaining to each user, the aggregate Trust index is subsequently obtained by taking in consideration this degree of ethical trust per user along with the experience of each user and ownership of each user. The calculated ethical trust index is distinctive in nature as it quantifies the hitherto qualitative concept of trust and ethics. Such a measure can significantly affect the market presence of the cloud provider in all situations. The prototype implementation of the algorithm provides an insight into the calculation procedure, which works by accepting inputs as factors which affect ethical trust on the cloud. Higher values of this index represent high ethical trust and lower values represent low ethical trust. The calculated ethical trust index values can be suitably customized and enhanced by considering more factors, in future.

References

1. Pearson, S., Charlesworth, A.: Accountability as a way forward for privacy protection in the cloud. In: Jaatun, M.G., Zhao, G., Rong, C. (eds.) CloudCom 2009. LNCS, vol. 5931, pp. 131–144. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10665-1_12
2. Haeberlen, A.: A case for the accountable cloud. SIGOPS Oper. Syst. Rev. **44**, 52–57 (2010). http://doi.acm.org/10.1145/1773912.1773926
3. van den Hoven, J.: Information technology, privacy and the protection of personal data. In: Information Technology and Moral Philosophy, pp. 301–321 (2008)
4. Timmermans, J., et al.: The ethics of cloud computing. In: Academia.edu (2010)
5. Nelson, M.: The cloud, the crowd, and public policy. Issues Sci. Technol. (2009). http://www.issues.org/25.4/nelson.html
6. Paquette, S., et al.: Identifying security risks associated with the governmental use of cloud computing. Gov. Inf. Q. (2010). ISSN 0740-624X
7. Alhamad, M., et al.: A trust-evaluation metric for cloud applications. Int. J. Mach. Learn. Comput. **1**(4) (2011)
8. Buyya, R.: Market-oriented cloud computing: vision, hype, and reality of delivering computing as the 5th utility. In: CCGRID 2009 Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid (2009)
9. Zeller, M., et al.: Open standards and cloud computing: Kdd-2009 panel report, pp. 11–18 (2009)
10. Chen, Y., et al.: What's New About Cloud Computing Security? (2010)
11. Capurro, R.: Privacy. An intercultural perspective. Ethics Inf. Technol. **7**, 37–47 (2005)

12. Shaikha, R., Sasikumar, M.: Trust model for measuring security strength of cloud computing. Proc. Comput. Sci. **45**, 380–389 (2015). International Conference on Advanced Computing Technologies and Applications (ICACTA)
13. Wang, Y.: Centroid defuzzification and the maximizing set and minimizing set ranking based on alpha level sets. Comput. Ind. Eng. 228–236 (2008)
14. Sharma, R., Trivedi, R.K.: Cloud computing–security issues, solution and technologies. Int. J. Eng. Res. **3**(4), 221–225 (2014)
15. Prajapati, S.K., et al.: Trust management model for cloud computing environment. In: Proceedings of the International Conference on Computing. Communication and Advanced Network - ICCCAN 2013 (2013)
16. Sharma, A., Banati, H. A framework for implementing trust in cloud computing. In: Proceedings of the International Conference on Internet of things and Cloud Computing. ACM DL (2016)
17. Ko, R.K.L., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., Lee, B. S.: TrustCloud: a framework for accountability and trust in cloud computing. In: 2nd IEEE Cloud Forum for Practitioners. IEEE (2011)
18. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. (2010). Elsevier
19. Sugeno, M.: An introductory survey of fuzzy control. Inf. Sci. (1985)
20. Lee, C.: Fuzzy logic in control systems: fuzzy logic controller, parts I and II. IEEE Trans. Syst. Man Cybern. (1990)