A User-Based Trust Model for Cloud Computing Environment

Othman Saeed[1], Riaz Ahmed Shaikh[2]
Computer Science Department
King Abdulaziz University
Jeddah, KSA

***Abstract*—There are many trust management models for the cloud environment. Selecting an appropriate trust model is not an easy job for a user. This work presents a new trust model called ARICA model which help a user to reduce the reliance on the trust value of provider and third-party feedback. Simultaneously, the ARICA model increases the dependence on the user trust value. Furthermore, the proposed model measured the trust based on five attributes: Availability, Reliability, Integrity, Confidentiality, and Authentication. This paper presents the comparison of the proposed ARICA trust model with two existing schemes. Results show that the proposed model provides better accurate results.**

Keywords*—Trust management model; trust value of provider feedback; trust value of third-party feedback; user trust value; availability; reliability; integrity; confidential; authentication

I. INTRODUCTION

Cloud computing is a service that is provided according to the request of the users. In addition, it can be accessed through network anytime. Furthermore, it provides computer resources that are independent of the user location, rapid flexibility, new usage patterns and new business features of IT technology. As a result of that, cloud computing has taken the attention of stakeholders and the researchers as an attractive model.

However, there are several disadvantages that make customers worried from using cloud computing technologies [1]. One of those improper characteristics is less control and less reliability. The biggest fear in any organization is to abandon the administrative responsibility to the external client such as cloud service provider. Moreover, security and privacy are one of the major cloud computing worries. These changes led researchers to find a trust management model which help consumers to control their data.

Lately, many trust management models in cloud computing have presented in the literature. In general, the system of the trust management model works as follows: first, consumers look for a service with good feedback. Next, the users will use this service and give their feedback. After that, cloud providers or third parties take the users' feedback and assess their services using some models. In the end, they save these feedback into the cloud provider database or/and into the third-party database that will be available for other users.

In this paper, the ARICA (Availability, Reliability, Integrity, Confidentiality, and Authentication) is presented. As compared to the existing models, the proposed model helps users to rely on two or three sources of databases (Provider feedback database - Third-party feedback database - User feedback database). Besides, the model will give the user feedback database more weight than the provider and\or third-party feedback database. Finally, the user will have all three sources of databases. However, the user can rely more on the source of their feedback because users trust their feedback more. There is a scenario in the fourth section to describe this situation in more detail.

The purpose of ARICA model is to help users relying on their feedback more than feedback from any other companies. Moreover, in the evaluation section, the proposed model gave remarkable results. In addition, this paper presents a comparison between the proposed model and two existing schemes (QoS-based Trust Model and FIFO-based trust model [32]). The comparison results (see Section 6) show that the ARICA model provided more accurate results to a user than those two schemes.

Rest of the paper is organized as follow. Section 2 presents literature work of three trust management models for cloud computing. A full description of the proposed model is described in Section 3. In Section 4, a scenario is presented to show the behavior of the ARICA model. Next, an experimental and discussion are given in Section 5. Section 6 shows a comparison and discussion between the proposed model and two other models. Section 7 concludes the paper and highlights some future work.

II. BACKGROUND

Bharathi *et al.* [2] have proposed an extended trust management scheme for cloud computing environment. It composed of four functions: 1) multi-attribute hashing function; 2) real-time service composition; 3) location based service selection; and 4) extended trust management scheme. Details of these functions are defined in very trivial manner. Their proposal is primarily used to verify the user's identity and authenticity. However, it cannot be used to verify the trust level of the cloud service providers.

Zhu *et al.* [3] claim that for different application scenarios, it is useful to integrate the wireless sensor networks with cloud computing environment. Due to resource constraints nature of sensor nodes, it is more feasible to store huge amount of sensory data in the cloud. Moreover, high-performance data

processing capability can also be utilized efficiently in the cloud. The authors have proposed a new authenticated trust and reputation calculation and management (ATRCM) system for cloud computing and wireless sensor network integration. The ATRCM system offers three functions. Firstly, it provides authentication service for cloud service providers and sensor network providers. This service is useful in mitigating malicious impersonation attacks. Secondly, it provides trust and reputation calculation mechanism for cloud and sensor network providers. Finally, cloud service users can select a suitable cloud service provider and it assists them to select an appropriate sensor network provider. The ATRCM system provides protection against good mouthing, bad-mouthing, collusion and white-washing attacks.

Xiao *et al.* [4] proposed a new methodology called attribute-driven. Furthermore, they applied a cloud ecosystem privacy and security within five attributes: 1) confidentiality; 2) integrity; 3) availability; 4) accountability; and 5) privacy-preservability. Furthermore, they focused on the weak relationships between these attributes that the attackers exploit. Moreover, they discussed the threat models and the weaknesses that can be exploited by opponents to proceed various attacks. Also, they talked about the defense strategies. Although several researchers considered privacy as a part of security, the authors extracted privacy from security because it's importance in cloud environments. However, some attack strategies are still not solved. In the end, this review will help researchers to guide their research in cloud security and privacy.

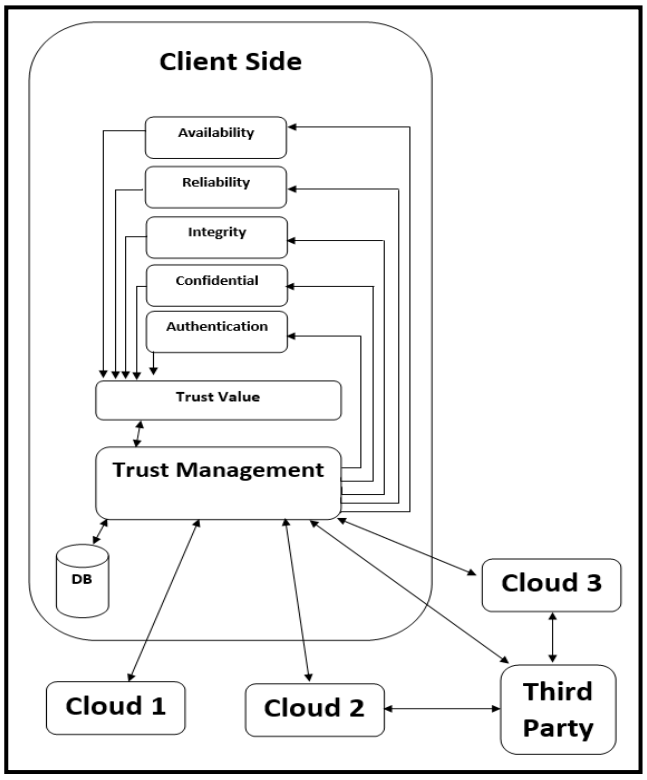

Fig. 1. ARICA model.

III. ARICA MODEL

Instead of depending on the provider feedback or the third-party feedback, the users can be based on their own evaluation or feedback of a particular cloud service. The proposed model helped the user to reduce the reliance on the trust value of provider and third-party feedback. At the same time, the model increases the dependence on the user trust value. As shown in Fig. 1, the proposed model measures the trust based on five attributes: Availability, Reliability, Integrity, Confidentiality, and Authentication.

A. Why these Five Attributes?

There are several attributes existing in the cloud that has been utilized by researchers. Those attributes promote clients to assess and manage the trust of the provider services. In this work, the five attributes (availability, reliability, confidentiality, integrity and authentication) are selected. The reason for selecting these attributes is that they are most commonly used in many recent research papers as shown in Table I.

TABLE I. PAPERS THAT USED SOME OF FIVE ATTRIBUTES

Paper Reference	Paper Year	Authentication	Availability	Reliability	Data Integrity	Confidential
[2]	2015		✔	✔	✔	
[3]	2015	✔				
[5]	2016	✔		✔		✔
[6]	2015	✔			✔	
[7]	2015		✔	✔	✔	✔
[8]	2015		✔	✔		
[9]	2016	✔				
[10]	2015	✔			✔	✔
[11]	2015	✔	✔			
[12]	2016	✔				
[13]	2015	✔	✔			✔
[14]	2015	✔				
[15]	2016		✔			✔
[16]	2016		✔			
[17]	2015	✔	✔		✔	✔
[18]	2016		✔	✔	✔	✔
[19]	2017			✔		
[20]	2016			✔		
[21]	2016				✔	
[22]	2016		✔	✔	✔	
[23]	2016				✔	
[24]	2015		✔	✔	✔	
[25]	2016		✔	✔		✔
[26]	2015		✔	✔		
[27]	2015		✔	✔	✔	
[28]	2015		✔	✔		
[29]	2015		✔			✔

There are many reasons which makes these attributes important, for example, without confidentiality, customer's information will have unlimited access from any user, and they will lose their privacy. Also, integrity gives consumers an insurance that their data is accurate and trustworthy. Furthermore, availability help users to access from anywhere to their data. Reliability describes the possibility of services to fulfill their required functions in a given time. However, without this quality, an environment will not have the desired confidence. In the end, if the authentication was abandoned, it is possible for any users to reach the information without restriction.

To summarize, the five attributes (availability, reliability, confidential, integrity and authentication) are desired for any cloud to acquire the users' trust. As shown in Table I, existing trust management schemes do not incorporate these five attributes all together.

B. Availability (Tv_1)

Availability is the possibility that a service will operate as ordered during a period of time. Equation (3) of Tv_1 is a division of two factors: 1) number of attempts that is accepted by a service (Av_c); and 2) the number of attempts submitted to the service (Se).

$$Av_c = \sum_{i=1}^{n}(Av_i) \quad (1)$$

$$Se = \sum_{i=1}^{n}(Se_i) \quad (2)$$

$$Tv_1 = \frac{Av_c}{Se} \quad (3)$$

Where *n* is the number of attempts on a service.

C. Reliability (Tv_2)

Reliability is the probability that a service will generate accurate results in a given time. Equation (5) of the reliability (Tv_2) is a division of two factors: 1) number of attempts accepted successfully by a service (Re_c); and 2) the number of attempts that is accepted by a service (Av_c)**.**

$$Re_c = \sum_{i=1}^{n}(Re_i) \quad (4)$$

$$Tv_2 = \frac{Re_c}{Av_c} \quad (5)$$

Where *n* is the number of attempts on a service.

D. Integrity (Tv_3)

Integrity is to keep data safe from intentional or unintentional data modification from unauthorized users. Moreover, it will emphasize the consistency and the accuracy of data across its lifecycle. The integrity (7) is calculated by dividing the number of attempts that data integrity is preserved by a service (6) with the number of attempts accepted successfully by a service (4).

$$In_c = \sum_{i=1}^{n}(In_i) \quad (6)$$

$$Tv_3 = \frac{In_c}{Re_c} \quad (7)$$

Where Re_c is the number of attempts accepted successfully by a service, In_c is the number of attempts that data integrity is preserved by a service, and *n* is the number of attempts on a service.

E. Confidentiality (Tv_4)

Confidentiality will keep the data of the consumer secret in the cloud system. In the proposed model, two parameters will be focused on: 1) the encrypting data that is traveling through the Internet between the cloud and the browser or the application added to 2) the encrypting data in the cloud as shown in (8).

$$Tv_4 = (EnApp * w_1) + (EnCl * w_2) \quad (8)$$

Where *EnApp* is the encrypting data that is traveling through the Internet between the cloud and the browser or the application, *EnCl* is the encrypting data in the cloud, and w_1 and w_2 are positive weights such that $w_1+w_2 = 1$.

F. Authentication (Tv_5)

Authentication confirms the consumer's right to access the information, and preserve the user's account from stealing identity and fraud. In the proposed model, the equation of authentication (9) uses four parameters [30], [31]: password-based, smart card based, one-time password-based and biometrics-based.

$$Tv_5 = \sum_{i=1}^{4}(A_i * w_i) \quad (9)$$

Where, A_1 is the password-based, A_2 is the smart card based, A_3 is the one-time password-based, A_4 is the biometrics-based, and w_1, w_2, w_3, and w_4 are positive weights such that $w_1+w_2+w_3+w_4 = 1$.

G. Trust Value Component (Tv)

This component is used to calculate the trust value between 0 and 1. Where, one means the service is fully trusted, and zero means the service is fully untrusted. The component will add these attributes: Availability, Reliability, Integrity, Confidentiality, and Authentication. At the same time, each attribute will multiply by its weight. At the end, the component will take the average by dividing the result by five as shown in (10).

$$Tv = \frac{1}{5}\sum_{i=1}^{5}(Tv_i * w_i) \quad (10)$$

Where Tv_1 is the Availability, Tv_2 is the Reliability, Tv_3 is the Integrity, Tv_4 is the Confidentiality, Tv_5 is the Authentication, and w_1, w_2, w_3, w_4, and w_5 are positive weights such that sum of all weight values equals to 1.

H. Database (DB)

The proposed model will create a separate record for each user in the DB. Furthermore, each record contains a trust value for each service that has been used by the user. Every time the customer uses a service, the ARICA model will produce a service evaluation value and store it in the user's DB. By this database, the model can rely on the trust value in the DB more than provider trust value or/and the third-party trust value.

I. Trust Management (TM)

In this section, trust management controls three trust values of the same service as shown in (11) (The Proposed Trust Value (*Tv*), Provider Trust Value (Tv_p) and Third-Party Trust Value (Tv_{tp})).

$$Tm = Tv * w_1 + Tv_p * w_2 + (\frac{1}{n} \sum_{i=1}^{n} (Tv_{tp\,i})) * w_3 \quad (11)$$

Where w_1, w_2, and w_3 are positive weights such that $w_1+w_2+w_3 = 1$.

These weights are based on the attempts of using the service. In addition, (n) in the equation is based on the number of third parties that voted for the same provider service. That means, if there are more than one third-party assess the provider service then Tv_{tp} will be the mean of the trust values of the third parties.

IV. Scenario

There are three main phases when a consumer uses the proposed model. The first one is when the trust management component deals with a provider and a third-party trust value more than the model trust value as shown in Fig. 2. The second phase is when the trust management component has a reliable trusted value in the database; it will deal the trust value in the database on the same level as the provider and the third-party trust value as shown in Fig. 3. Finally, the trust management component deals with the model trust value more than the provider, and a third-party trust value as shown in Fig. 4.

A. First Phase

1) When the customer starts using the service *A* of the cloud provider *P*, the model will rely on the *P* feedback or/and with the third-party of *P* feedback.

2) Then, the model will calculate the trust value of *A* by using the five attributes (Availability, Reliability, Integrity, Confidential and Authentication).

3) After that, in the trust value component, the model will take the trust values and calculate the trust value and send it to the trust management component.

4) Next, the trust management component will save the trust value of *A* in the database.

5) At the end, the trust management component will calculate the total trust value by using the trust value from the model and from *P* and third party of *P*.

6) The model in this phase will rely more on the cloud provider and third-party feedback as shown in Fig. 2.

Fig. 2. Less priority on the model trust value.

B. Second Phase

1) After repeating the first phase, the service *A* will have numbers of trust values saved into the database. These trust values will build good experience of *A*.

2) By the time, the background of the database will be increased.

3) As a result, the trust management component will reduce the priority of the *P* trust value and the third party of *P* trust value.

4) At the same time, the priority of trust value of will be increased as shown in Fig. 3.

Fig. 3. Same level of priority on both trust values.

C. Third Phase

1) By the time, the model will repeat the second phase till the database gets the adequate experience of *A*.

2) The model in this phase will rely more on model trust value as shown in Fig. 4.

Fig. 4. More priority on the model trust value.

V. Experiment and Discussion

The experiments in this study have not been applied to a particular cloud.

Instead of all that, random datasets were used on the proposed model. The reason for that is the unavailability of real world dataset(s). The ten datasets of random 1000 feedbacks are used in the system. These 10 datasets are available online[1]. In each experiment, the mean of 10 datasets was taken. So, each experiment had a dataset of 1000

[1] https://drive.google.com/file/d/0B_mWyE7-E0r8b0xGc21SOHUxRWk5Y041MmJOS0h0Vjc4UHhR/view?usp=drivesdk

feedbacks. Each feedback value was between 1 (trusted value) and 0 (untrusted value).

As mentioned in the introduction that there are three sources of databases (Provider feedback database – Third-party feedback database – User feedback database). This section presents the use case scenarios of these three databases.

There are four trust values in this experiment:

- Trust management value Tm (user feedback database): this value is the outcome feedback from ARICA model. Moreover, this value will send back to the provider or/and to third-party as the user feedback. In addition, it will be saved into the user feedback database.
- Trust value of provider TVP (Provider feedback database): this value will be taken from the provider.
- Trust value of third-party TVTP (Third-party feedback database): this value will be taken from the third-party.
- Trust value of the model TVM (Trust Value Component (*Tv*)): this value is the outcome from Trust Value Component (*Tv*).

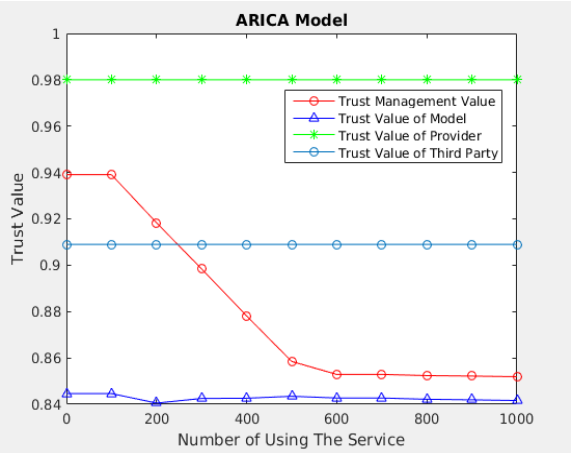

Fig. 5. The results of the first experiment.

The first test made on a service in cloud[1]. The results are shown in Fig. 5. There were two evaluation values for this service. One value was taken from a provider feedback database. This value was 0.98 in the first test. The other value was taken from a third-party feedback database. This value was 0.91 in the first test. After using the service 1000 times the user found that the outcome of Trust Value Component (*Tv*) was between 0.843 and 0.840. Trust Management (*Tm*) component gave the mean of TVP and TVTP high weight (0.8). On the other hand, the weight of TVM was (0.2). After 100 times of using the service, the Tm started to increase the weight of TVM to 0.4. At the same time, Tm decreased the weight of mean value to 0.6 and so on. After 500 times of using the service, the weight of TVM becomes steady on 0.8 while the weight of the mean value was 0.2. In Fig. 6 there are:

1) Trust Value of Provider (TVP) (The weight = 0.8)
2) Trust Management Value (*Tm*) (The manager)
3) Trust Value of the Model (TVM) (The weight = 0.2)

The steps of changing the weights are given below:

1) Slightly, *Tm* decreased the weight of TVP.
2) In the same time, Tm increased the weight of TVM.
3) This process stopped if the weight of TVP = 0.2 and the weight of TVM = 0.8

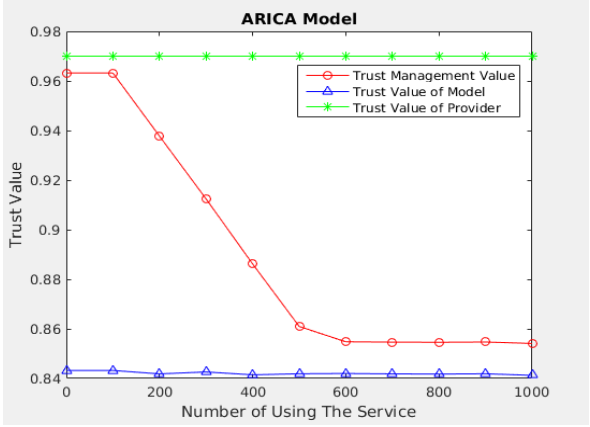

Fig. 6. The results of the second experiment.

In Fig. 7 there are:

1) Trust Value of Provider (TVP)
2) Four Trust Value of Third-parties (TVTP)
3) Trust Management Value (Tm) (The manager)
4) Trust Value of the Model (TVM) (The weight = 0.2)

The steps of changing the weights are given below:

1) Before the *Tm* started, it took the mean of the four TVTPs.
2) After that, *Tm* took the total mean of TVP and the mean of the four TVTPs.
3) Next, *Tm* set the weight of the total mean to 0.8
4) Slightly, *Tm* decreased the weight of the total mean.
5) In the same time, *Tm* increased the weight of TVM.
6) This process stopped if the weight of the total mean = 0.2 and the weight of TVM = 0.8

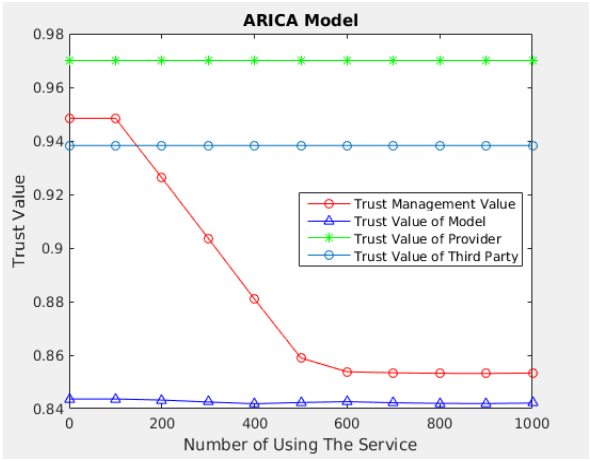

Fig. 7. The results of the third experiment.

These result shows that provider and the third-party feedback database are not reliable because they gave untrusted feedback as compared to user feedback database. Perhaps the reason for these unreliable feedbacks from the providers was that companies wanted to get a large number of customers to distribute their services. These results help users to decide whether to use this service or to choose another cloud provider.

VI. Comparison and Discussion

In this section, the comparison of the proposed model with existing two schemes is presented in two different scenarios. The process of using dataset in this section is the same as the experimental section. That's mean, 10 datasets of random 1000 feedbacks were used in each comparison.

The proposed model is compared with the following two models:

1) Quality of service-based model (QoS based model): Paul Manuel [32] has proposed a new trust model for a cloud resource called QoS Trust model. It is based on four qualities of service parameters, which are: reliability (RE), availability (AV), turnaround efficiency (TE), and data integrity (DI). In order to compute trust, the author has first assigned different weight values (w_1, w_2, w_3, and w_4) for each parameter and then sums them all together in the following manner: w_1*AV+ w_2*RE + w_3*DI+ w_4*TE. Author has compared the proposed QoS trust model with the FIFO model and combined trust model. The experimental results indicate that the QoS trust model performs better than the FIFO model and combined trust model. Author has also provided an architecture for the trust management system that can be used to measure the trust value of the different cloud resources. It also contains details about trust repository, catalog service, and cloud coordinator etc. More QoS parameters like utilization, accountability. auditability any much more can be included in this model.

2) First-in-first-out model (FIFO model): this model is not fully trusted. When a user asks for a service, he/she will get this service whether it is trusted or not trusted. This kind of process is risky.

The dataset of availability, reliability, and data integrity are the same for each comparison. These three attributes have different weight in ARICA model and in QoS based model. The three attributes were equalized to get a fair comparison. The confidential, authentication (in ARICA model) and turnaround efficiency (in QoS based model) were not the same for each comparison. The difference on these three attributes was based on the service level agreement (SLA) between a consumer and a provider. The FIFO model had the same results in all comparison. The three comparisons are below:

A. First Comparison

The first comparison made on a service *A, which* provides the following features: encrypting data through the Internet, encrypting data in the cloud, password-based, smart card based, one-time password-based and biometrics-based authentication. The turnaround efficiency of service *A* was always same as stated in the SLA. That means the turnaround efficiency was one (trusted) in every test.

This SLA was assumed to give the ARICA model and QoS based model the best possible performance. The value of each model's attribute is given below. Furthermore, the results of this comparison are in Fig. 8.

For the first comparison, the ARICA model was configured in the following manner:

- The weight of the **availability** is 0.2
- The weight of the **reliability** is 0.2
- The weight of the **data integrity** is 0.2
- The weight of the **confidential** is 0.2
  - The weight of encrypting data through the Internet is 0.8 (Exist)
  - The weight of **encrypting data in the cloud** is 0.2 (Exist)
- The weight of the **authentication** is 0.2
  - The weight of **password-based** is 0.7 (Exist)
  - The weight of **smart card based** is 0.2(Exist)
  - The weight of **one-time password-based** is 0.05 (Exist)
  - The weight of **biometrics-based** is 0.05 (Exist)

The service-based model was configured in the following manner:

- The weight of the **availability** is 0.3
- The weight of the **reliability** is 0.23
- The weight of the **data integrity** is 0.17
- The weight of the **turnaround efficiency** is 0.3 (Always One)

For the FIFO model, all that a provider gives to the user, the user will take it either it is trusted or not.

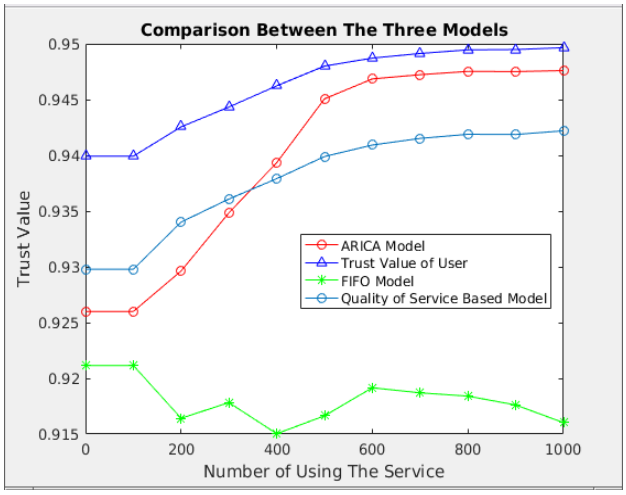

Fig. 8. The results of the first comparison.

As shown in Fig. 8 the ARICA model gave results between QoS based model and FIFO model. After testing service *A* 500 times[2], the ARICA model increased and get near to the results of the trust value of the user. The trust value of the user was calculated by ARICA model.

At the end of this comparison, ARICA model generates better results than the QoS based model. This was because ARICA model had more attributes than the QoS based model.

B. Second Comparison

The second comparison made on a service B. SLA of service B provided encrypting data through the Internet, password-based and smart card based. As in the first comparison, the turnaround efficiency of service B was one (trusted) in every test.

This SLA was assumed to make the results of QoS based model much better than the trust value results of the user to see the behavior of ARICA model. The value of each model's attribute is given below. Furthermore, the results of this comparison are shown in Fig. 9.[3]

For the second comparison scenario, the ARICA model was configured in the following manner:

- The weight of the **availability** is 0.2
- The weight of the **reliability** is 0.2
- The weight of the **data integrity** is 0.2
- The weight of the **confidential** is 0.2
  - The weight of encrypting data through the Internet is 0.8 (Exist)
  - The weight of **encrypting data in the cloud** is 0.2 (Not Exist)
- The weight of the **authentication** is 0.2
  - The weight of **password-based** is 0.7 (Exist)
  - The weight of **smart card based** is 0.2(Exist)
  - The weight of **one-time password-based** is 0.05 (Not Exist)
  - The weight of **biometrics-based** is 0.05 (Not Exist)

The following values were assumed for quality of service-based model:

- The weight of the **availability** is 0.3
- The weight of the **reliability** is 0.23
- The weight of the **data integrity** is 0.17
- The weight of the **turnaround efficiency** is 0.3 (Always One)

For the FIFO model, we used the same assumption which was taken in the first scenario,

The reason for the decline of ARICA model's results in Fig. 9 was that the SLA of service *B* didn't meet the user requirements. Furthermore, The ARICA model was between QoS based model and FIFO model. After 500 times of testing service *B*, the ARICA model got adequate experience to decrease and become near to the results of the trust value of the user.

In the end of this comparison, ARICA model was better than QoS based model and FIFO model. The result of that was ARICA model met the user trust results.

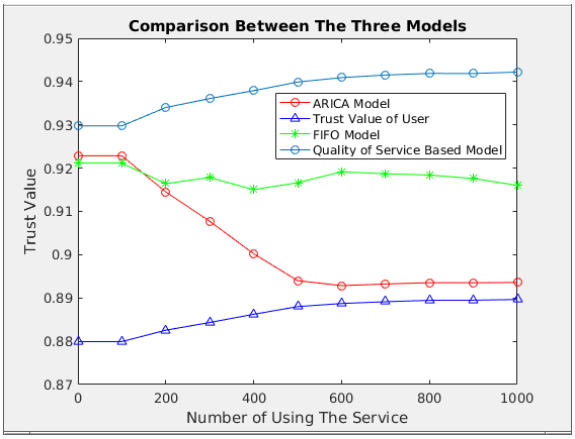

Fig. 9. The results of the second comparison.

C. Third Comparison

This comparison made on a service *C* and on different SLA. This agreement included encrypting data through the Internet, encrypting data in the cloud, password-based and smart card based. The turnaround efficiency of service *C* was fluctuated from time to time. That means the turnaround efficiency wasn't always the same as the time in SLA of service *C*.

This SLA was assumed to make the results of the turnaround efficiency in QoS based model inconsistent. Furthermore, the results of this comparison are in Fig. 10.[4]

The values of ARICA model used for this scenario were:

- The weight of the **availability** is 0.2
- The weight of the **reliability** is 0.2
- The weight of the **data integrity** is 0.2
- The weight of the **confidential** is 0.2
  - The weight of encrypting data through the Internet is 0.8 (Exist)

[2] The dataset is available online: https://drive.google.com/file/d/0B_mWyE7-E0r8dEtQZmpBeHpJLTAwYzdRQUJRUl80eTk2MlNj/view?usp=drivesdk

[3] The dataset is available online: https://drive.google.com/file/d/0B_mWyE7-E0r8QWxyYnZJTGpvV2k3QldHN3ZPeEY1N2RSN0Jj/view?usp=drivesdk

[4] The dataset is available online: https://drive.google.com/file/d/0B_mWyE7-E0r8Q1ZyMGtWa2hBYi1SSloxWVA0UHBHcUF0ZWln/view?usp=drivesdk

- The weight of **encrypting data in the cloud** is 0.2 (Exist)

- The weight of the **authentication** is 0.2
  - The weight of **password-based** is 0.7 (Exist)
  - The weight of **smart card based** is 0.2(Exist)
  - The weight of one-time password-based is 0.05 (Not Exist)
  - The weight of biometrics-based is 0.05 (Not Exist)

The values of quality of service-based model:

- The weight of the **availability** is 0.3
- The weight of the **reliability** is 0.23
- The weight of the **data integrity** is 0.17
- The weight of the **turnaround efficiency** is 0.3 (Randomly)

The values of FIFO model: All that a provider gives to the user, the user will take it either it is trusted or not.

From the SLA of service *C*, the trust values of the user were better than QoS based model values and FIFO model values. As a result, ARICA model values increase. In this comparison, ARICA model was the better model that represented the trust results of the user.

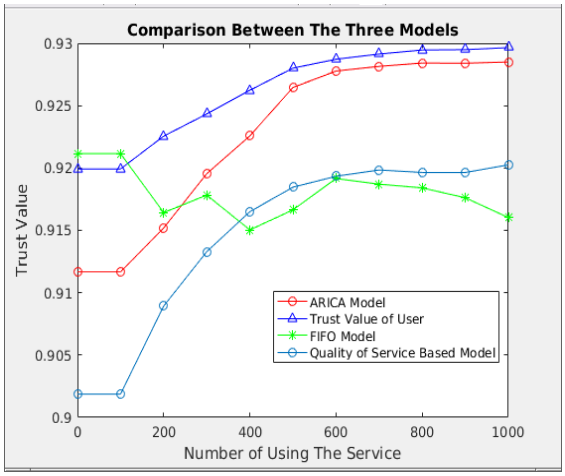

Fig. 10. The results of the third comparison.

D. Fourth Comparison

This comparison made on a service *D* and on various SLA. This service did not offer any confidentiality and authentication support. The turnaround efficiency of service *D* was the same as the turnaround efficiency of service *C* in the previous comparison. This assumption was presented to test the ARICA model in almost the worst scenario to see the reaction of this model.

The values of ARICA model:

- The weight of the **availability** is 0.2
- The weight of the **reliability** is 0.2
- The weight of the **data integrity** is 0.2
- The weight of the **confidential** is 0.2
  - The weight of encrypting data through the Internet is 0.8 (Not Exist)
  - The weight of **encrypting data in the cloud** is 0.2 (Not Exist)
- The weight of the **authentication** is 0.2
  - The weight of **password-based** is 0.7 (Not Exist)
  - The weight of **smart card based** is 0.2(Not Exist)
  - The weight of **one-time password-based** is 0.05 (Not Exist)
  - The weight of **biometrics-based** is 0.05 (Not Exist)

The values of quality of service-based model:

- The weight of the **availability** is 0.3
- The weight of the **reliability** is 0.23
- The weight of the **data integrity** is 0.17
- The weight of the **turnaround efficiency** is 0.3 (Randomly)

The values of FIFO model:

All that a provider gives to the user, the user will take it either it is trusted or not.

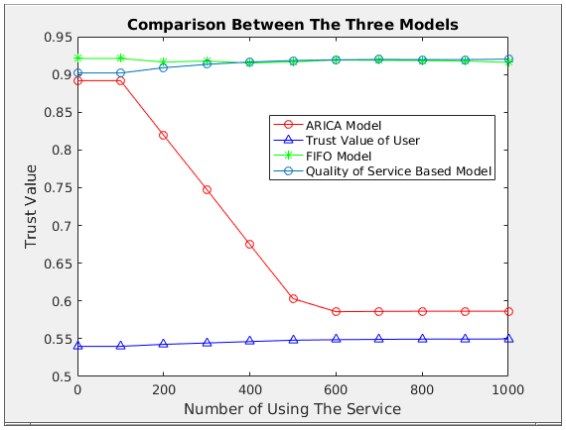

Fig. 11. The results of the fourth comparison.

In Fig. 11,[5] the trust values of ARICA model were sharply decreased because of the trust values of the user. The result of these low values was the SLA of service *D* did not meet the user requirements. Moreover, The ARICA model was in the middle of QoS based model and FIFO model. Next, the ARICA model got enough experience to decline and become close to the results of the trust value of the user after 500 times of testing service *D*.

[5] The dataset is available online: https://drive.google.com/file/d/0B_mWyE7-E0r8OUVReDFSNUJQNVVMaXlocTlLclVEQTREUkJV/view?usp=drivesdk

At the end of this comparison, ARICA model was better than QoS based model and FIFO model. The results of ARICA model were meeting the user trust results. After that, the user can decide whether to continue using this service or no.

VII. Conclusion and Future Work

From the comparison, the ARICA model always relied on the trust results of a user. Therefore, ARICA model produced more reliable results than QoS based model and FIFO based model. The proposed ARICA model designed to promote users to rely on different database sources (Provider feedback database – Third-party feedback database – User feedback database). Initially, the model gave the user feedback database more weight than the other two databases. This process continued until the user database feedback get adequate experience. In the end, the user relied on his/her database rather than the provider or/and the third-party database.

With the help of five attributes (Availability, Reliability, Integrity, Confidential and Authentication), the ARICA model gives users the ability to control their data. As a result, the model reduces the fear of customers from using cloud computing technology.

In the future work, to make the model more flexible, the weights will be distributed on the three feedback databases according to the benefit of the business. Also, the model will be tested on a real cloud environment to get more accurate results.

References

[1] Noor, Talal H., Quan Z. Sheng, Sherali Zeadally, and Jian Yu,"Trust management of services in cloud environments: Obstacles and solutions." *ACM Computing Surveys (CSUR)* 46.1 (2013): 12.

[2] Bharathi, C., V. Vijayakumar, and K. V. Pradeep. "An Extended Trust Management Scheme for Location Based Real-time Service Composition in Secure Cloud Computing." *Procedia Computer Science* 50 (2015): 103-108.

[3] Zhu, C., Nicanfar, H., Leung, V. C., & Yang, L. T. "An authenticated trust and reputation calculation and management system for cloud and sensor networks integration." *Information Forensics and Security, IEEE Transactions on* 10.1 (2015): 118-131.

[4] Xiao, Zhifeng, and Yang Xiao. "Security and privacy in cloud computing." *Communications Surveys & Tutorials, IEEE* 15.2 (2013): 843-859.

[5] Shapiro, D., Socher, M., Lei, R., Muralidhar, S., Loo, B. T., & Heninger, N. "Daruma: Regaining Trust in Cloud Storage." (2016).

[6] Shaikh, Rizwana, and M. Sasikumar. "Trust model for measuring security strength of cloud computing service." *Procedia Computer Science* 45 (2015): 380-389.

[7] Monir, M. B., AbdelAziz, M. H., AbdelHamid, A. A., & EI-Horbaty, E. S. M. "Trust management in cloud computing: A survey." Intelligent Computing and Information Systems (ICICIS), 2015 IEEE Seventh International Conference on. IEEE, 2015.

[8] Namal, S., Gamaarachchi, H., MyoungLee, G., & Um, T. W. "Autonomic trust management in cloud-based and highly dynamic IoT applications." ITU Kaleidoscope: Trust in the Information Society (K-2015), 2015. IEEE, 2015.

[9] Bhardwaj, Akhilesh Kumar, and Rajiv Mahajan. "TTP based vivid protocol design for authentication and security for cloud." Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on. IEEE, 2016.

[10] Yan, Zheng, Peng Zhang, and Athanasios V. Vasilakos. "A security and trust framework for virtualized networks and software-defined networking." Security and communication networks 9.16 (2016): 3059-3069.

[11] Choudhary, Sapna, Amarjeet Kurmi, and Abhishek Dubey. "Monitoring Cloud Resources Based on SAAS Community using Cloud Bee Live Cloud Service." (2015).

[12] Nagaraju, Sabout, and Latha Parthiban. "SecAuthn: Provably secure multi-factor authentication for the cloud computing systems." Indian Journal of Science and Technology 9.9 (2016).

[13] Tang, Bo, Ravi Sandhu, and Qi Li. "Multi-tenancy authorization models for collaborative cloud services." Concurrency and Computation: Practice and Experience 27.11 (2015): 2851-2868.

[14] Wu, L., Zhou, S., Zhou, Z., Hong, Z., & Huang, K. "A Reputation-based identity management model for cloud computing." Mathematical Problems in Engineering 2015 (2015).

[15] Noor, T. H., Sheng, Q. Z., Yao, L., Dustdar, S., & Ngu, A. H. "CloudArmor: Supporting reputation-based trust management for cloud services." IEEE transactions on parallel and distributed systems 27.2 (2016): 367-380.

[16] Jabbar, S., Naseer, K., Gohar, M., Rho, S., & Chang, H. "Trust model at service layer of cloud computing for educational institutes." The Journal of Supercomputing 72.1 (2016): 58-83.

[17] Bernabe, Jorge Bernal, Gregorio Martinez Perez, and Antonio F. Skarmeta Gomez. "Intercloud trust and security decision support system: an ontology-based approach." Journal of Grid Computing 13.3 (2015): 425-456.

[18] Alabool, Hamzeh Mohammad, and Ahmad Kamil Bin Mahmood. "A novel evaluation framework for improving trust level of Infrastructure as a Service." Cluster Computing 19.1 (2016): 389-410.

[19] Selvaraj, Alagumani, and Subashini Sundararajan. "Evidence-Based Trust Evaluation System for Cloud Services Using Fuzzy Logic." International Journal of Fuzzy Systems 19.2 (2017): 329-337.

[20] Raja, Sivakami, and Saravanan Ramaiah. "2S-FAT-Based DLS Model for Cloud Environment." Arabian Journal for Science and Engineering 41.8 (2016): 3099-3112.

[21] Pinheiro, Alexandre, Edna Dias Canedo, Rafael Timóteo de Sousa Jr, and Robson de Oliveira Albuquerque. "A Proposed Protocol for Periodic Monitoring of Cloud Storage Services Using Trust and Encryption." In International Conference on Computational Science and Its Applications, pp. 45-59. Springer International Publishing, 2016.

[22] Huang, Qiang, Dehua Zhang, Le Chang, and Jinhua Zhao. "Building Root of Trust for Report with Virtual AIK and Virtual PCR Usage for Cloud." Security, Privacy, and Anonymity in Computation, Communication, and Storage: 9th International Conference, SpaCCS 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings 9. Springer International Publishing, 2016.

[23] Boopathy, D., and M. Sundaresan. "Secured Cloud Data Storage—Prototype Trust Model for Public Cloud Storage." Proceedings of International Conference on ICT for Sustainable Development. Springer Singapore, 2016.

[24] Filali, Fatima Zohra, and Belabbes Yagoubi. "Global trust: a trust model for cloud service selection." International Journal of Computer Network and Information Security 7.5 (2015): 41.

[25] Ma, Zifei, Rong Jiang, Ming Yang, Tong Li, and Qiujin Zhang. "Research on the measurement and evaluation of trusted cloud service." Soft Computing (2016): 1-16.

[26] Namal, Suneth, Hasindu Gamaarachchi, Gyu MyoungLee, and Tai-Won Um. "Autonomic trust management in cloud-based and highly dynamic IoT applications." ITU Kaleidoscope: Trust in the Information Society (K-2015), 2015. IEEE, 2015.

[27] Filali, Fatima Zohra, and Belabbas Yagoubi. "A General Trust Management Framework for Provider Selection in Cloud Environment." East European Conference on Advances in Databases and Information Systems. Springer International Publishing, 2015.

[28] Rajendran, V. Viji, and S. Swamynathan. "Hybrid model for dynamic evaluation of trust in cloud services." Wireless Networks 22.6 (2016): 1807-1818.

[29] Fan, Wen-Juan, Shan-Lin Yang, Harry Perros, and Jun Pei. "A multi-dimensional trust-aware cloud service selection mechanism based on evidential reasoning approach." International Journal of Automation and Computing 12.2 (2015): 208-219.

[30] Reshmi, G., and C. S. Rakshmy. "A survey of authentication methods in mobile cloud computing." 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, 2015

[31] Bhatia, Tarunpreet, and A. K. Verma. "Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues." The Journal of Supercomputing (2017): 1-74.

[32] Manuel, Paul. "A trust model of cloud computing based on Quality of Service." *Annals of Operations Research* 233.1 (2015): 281-292.