Trusted Cloud Certifying Authority for Cloud Security

Mahesh Kalyanaraman
Corporate Security Team, Tata Communications Limited.

Received: June 05, 2018 Accepted: July 28, 2018

ABSTRACT *Now a day's cloud computing is becoming progressively popular in IT. It helps to provide elasticity and flexibility to fulfil the condition of current companies in computing properties and services. Cloud computing has deals with dynamic, shared service, scalable and cost-effective for enterprises. However, the problem of trusting the cloud computing is a supreme concern for enterprises as trust is widely noted as the top problems for the approval and improvement of cloud computing. To achieve this, trust should be established between Cloud Service Provider (CSP) and Cloud Consumer (CC).This research work mainly focuses on the design of trust-based model to control the uncertainty and vulnerability issues caused by both CSP and consumers, in order to rate the cloud service provider and consumer based on the trust score,a model is proposed with Recommendation System (RS) technique.In the cloud trust authority module will seek data input from authoritative sources based on the security parameter and it runs in the Collaborative Filtering algorithm (CF).Trust score on a real time basis without recreating a duplicate data base of its source data is done by Trusted Cloud Certifying Authority (TCCA).*

Keywords: *Cloud computing,Cloud Service Providers (CSP),Cloud Consumer (CC),Cloud Trust Authority,Trust Scoring, Rating, Trusted Cloud Certifying Authority (TCCA)*

1. Introduction

Cloud computing is mainly used for sharing the storage resources between multiple users or computational units. It provides a successful to theconsumers with very strong computational capability used in information technology over the network as a service and huge memory space at low cost. With the advent of advanced software and network technologies, it can provide various levels of services and enable the completion of different tasks over the Internet.In the ever-expanding cloud computing arena, where in the physical and logical boundaries are completely alienated and no face attached between the consumer and the service providers, TRUST becomes a key concern. The key stake holders in the environment are

1. Cloud Service Providers
2. Enterprise Consumers
3. Individual Consumers

1.1 The need of the TRUST in the Cloud Computing environment

In the case of the traditional computing environment, the consumer knows whois his service provider and there exists certain relationships between the parties. Both the parties know each other on the other side. So, kinds of relationship which in a way act like a trust between the service provider and the consumer. But in the present-day scenario as more and more organizations irrespective of the nature of the business and the risk involved in the business are migrating to leverage the cost economics, the trend of adoption of cloud technologies for sure is going to increase in the coming years and industry is not ready to look back.

With the increasing trend of adoption of cloud technologies, it becomes a challenge to understand how

- The cloud service provider is providing the services to his customer in a secure manner not impacting the availability,confidentiality and integrity along with maintaining the reputation of the service provider.
- If a reseller is involved in selling the services of cloud service provider, the relationship and the trust between cloud service provider and the consumer is debatable.

  Also, the reputation of the consumers in this case can the either the individual consumers or the enterprise consumers is also a cause of concern for the service provider. Themain focus of this paper is about design of trust-based model to control the uncertainty and vulnerability issues caused by the authorization, in order to rate the cloud service provider and consumer based on the trust score. This model is proposed with Recommendation System (RS) technique. RS is mainlyorganized towards individuals or users who have lack of sufficient experience or capability to evaluate services of the CSP. RS can offer personalized recommendations as ranked lists of the services by predicting the most suitable services, based on the preferences and constraints specified by the user.RS leverages the recommendations produced by a community of cloud users to provide recommendations to users looking for suggestions. This approach is termed as

Collaborative Filtering (CF) that can be either based on user-user collaboration or service-service collaboration. CF is classified as memory-based and item-based techniques whereas memory-based CF predicts the rating of active users based on the rating of the similar users and item-based CF predicts the rating based on the information about the items similar to the items chosen by the user. In this research the proposed technique used as memory-based technique. This approach uses user rating data to compute the correlation between users (consumer) or items (security parameters). Pearson correlation coefficient is used to calculate the similarity between users, and predicts the security values of both cloud services and consumers.

2.Literature Review

Rizwana Shaikh and Dr. M. Sasikumar[1] the authors has created a framework which evaluates the cloud service provider based on defined parameters mapping to the features and specifications offered as a service by the cloud service provider. Usvir Kaur and Dheerendra [2] provides framework for a trust model covering the cloud service provider and the users. This covers the parameters like identity management systems, authorization, authentication, data protection, confidentiality, communication and isolation. The trust model is built around cloud user, cloud service provider and cloud service specifications. K. Gokulnath and RhymendUthariaraj [3] haveexplored the offered solutions for cloud trust and facilitate with a rigid solution to accomplish the issue in future. Zhu C et al.,[4] discusses that direct method trust value can be calculated only if the system has the transactional history with the service provider. In several instances cloud consumers may not have any transactional history with the cloud service provider. In these instances system with transactional history over service providers are considered. With additional conditions in apart from trust calculation, reputation of the recommender system is evaluated. A.Logeshwari et al.,[5] in their paper has presented about privacy protection and data security issues in cloud computing, and those issues that prevent the people from using the cloud and provide the solutions which has done to reduce the risks and issues. Sianipearson [6] has described the evaluation of issues namely security, privacy and trust which occur in the background of cloud computation the technique in which it may be addressed. Anupam Das and Mohammad Mahfuzul [7] has analyzed in their paper with various factors associated to estimate the trust as an agent and have proposed a complete quantitative model for the measurement of trust and new load balancing algorithm according to various defined factors in the model. Zheng yan and Christian prehofer[8] has proposed a model as adaptive trust control to indicate, evaluate, ensure and establish the relationship of trust with system entities. The model has interest in quality attributes of entity and number of trust control modes of supported by the system. Islam Noor et al.,[9] design and implementation of Cloud Armor. Wang et al.,[10]proposed to solve the trust evaluation of cloud services. Li et al.,[11] represents the credibility of providers and also apply the fuzzy comprehensive evaluation method to classify the services. Sultan Aldossary and William Allen[12] have proposed in order to protecting people by endorsing the cloud and present a survey on solutions which has done to minimize the risks of these issues. Banirostam et al., [13] describe to make the cloud computing infrastructures reliable for ordering developers to provide closed execution environment. Shaikh and SasiKumar [14] have proposed to access the security of a service and validity of the model. Sidhu and Singh[15] discusses how to calculating the trust worthiness of service providers and users. Habib et al.,[16]describes the order to verify and evaluate security controls by first considering consumers' requirement. Fan, et al.,[17] in their paper proposes the system operational performance, Quality of Service (QoS). Abbadi and Alawneh [18] identify the related challenges for establishing trust in the cloud.

3. Research Methodology

The study utilized Recommendation System (RS) technique is to address the trust score using security parameter. This research uses surveys/questionnaire which is capable of illustrating adequate information about the trust service provider and the consumer which can be analyzed easily.

3.1 Approach to Research Design

The study was designed to consist of the following four phases as shown in Figue.1 below

Phase I: Information collection phase

During this phase, sample used for the research consists of 140 consumers with various service provider which is confidential so, dataset is provided for Cloud Service Provider (CSP) with CSP1, CSP2 etc.cloud consumer. This relevant datasets are prepared based on the questionnaires prepared which illustrate the information security parameters for cloud service provider, consumer and consumer's cybersecurity team along with its environment. These questionnaires are made to focus about security related parameters

regarding cloud computing security, storage, speed, data privacy, real time monitoring and management, service quality and performance of cloud infrastructure in their companies and also for individual consumers.

Phase II: Identification of security parameters for trust score

The datasets consist of enormous variables initiated from the available questionnaires which are the feedback of cloud service provider, individual consumer from their organization and as well as general individual consumer about the cloud environment and the cloud service provider. In order to accomplish the trust score for the cloud service provider by rating the parameter which related to the security, data privacy and safety. The major parameters related to this trust score of the cloud service provider are confidentiality, identity management, reliability, reputation, privacy, service level agreements and transparency. The security parameters are the key role parameter for security incidents, legal and regulatory issues, security incident and criminal background. In order to achieve the best trust score or ranking, any cloud service provider has to stick with these security parameter as well as consumer has good ranking score and which cloud service provider can provide service.

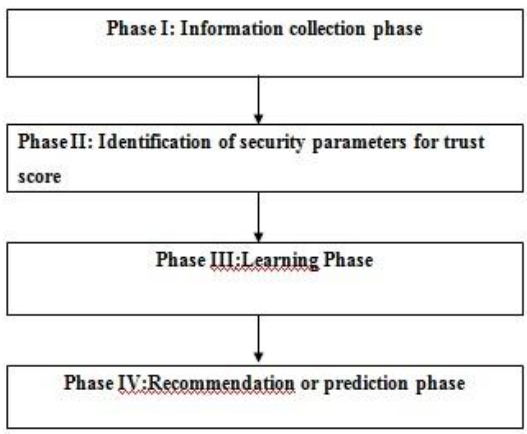

Figure.1 Phases of Research

Phase III: Learning phase

The cloud trust authority module will seek data input from authoritative sources based on the security parameter which runs the Collaborative Filtering algorithm (CF).CF is the process of predicting the rating score of the cloud user on the basis of rating of the services. CF technique works by creating a user-service matrix of preferences for services by users. It matches users with relevant interest and preferences by calculating the similarities between their profiles to make recommendations. It is classified as memory-based and item-based techniques. In this research the proposed technique used as memory-based technique. This approach uses user rating data to compute the similarity between users (consumer) or items (security parameters). Pearson correlation coefficient is used to calculate the similarity between users, and predicts the security values of both cloud services and consumers.

Phase IV: Recommendation or prediction phase

The cloud service with the best trust score is chosen for recommendation, on the basis of security parameter. In order to accomplish the predictive rating score of the cloud user on the basis of probability of service recommended to the user. Finally, the prediction phase generates the results according to the similarity measure and user preferences. The decisions are made using the user profiles constructed in the information gathering phase, which is used as a training set in the learning phase.

3.2 Trusted Cloud Certifying Authority (TCCA)

The Trust Score will be published by the Cloud Trust Authority which can be accessed by either the cloud service provider or the cloud consumer. Below are the lists of sources identified from whom TCCA will seek inputs for the identified security parameter to arrive at the trust score.

1. Aadhar Database from UIDAI, Government of India
2. PAN Database from Department of Income Tax, Government of India
3. National Crime Record Database, Department of Home Affairs, Government of India
4. Registrar of Companies Database, Department of Company Affairs, Government of India
5. Passport and Immigration database, Department of Foreign Affairs, Government of India
6. Interpol Red Corner Database for notified criminals including drug trafficking and Child Pornography, Interpol
7. Internet Watch guard groups databases like Phishtank, Spamhaus, Google Transparency etc

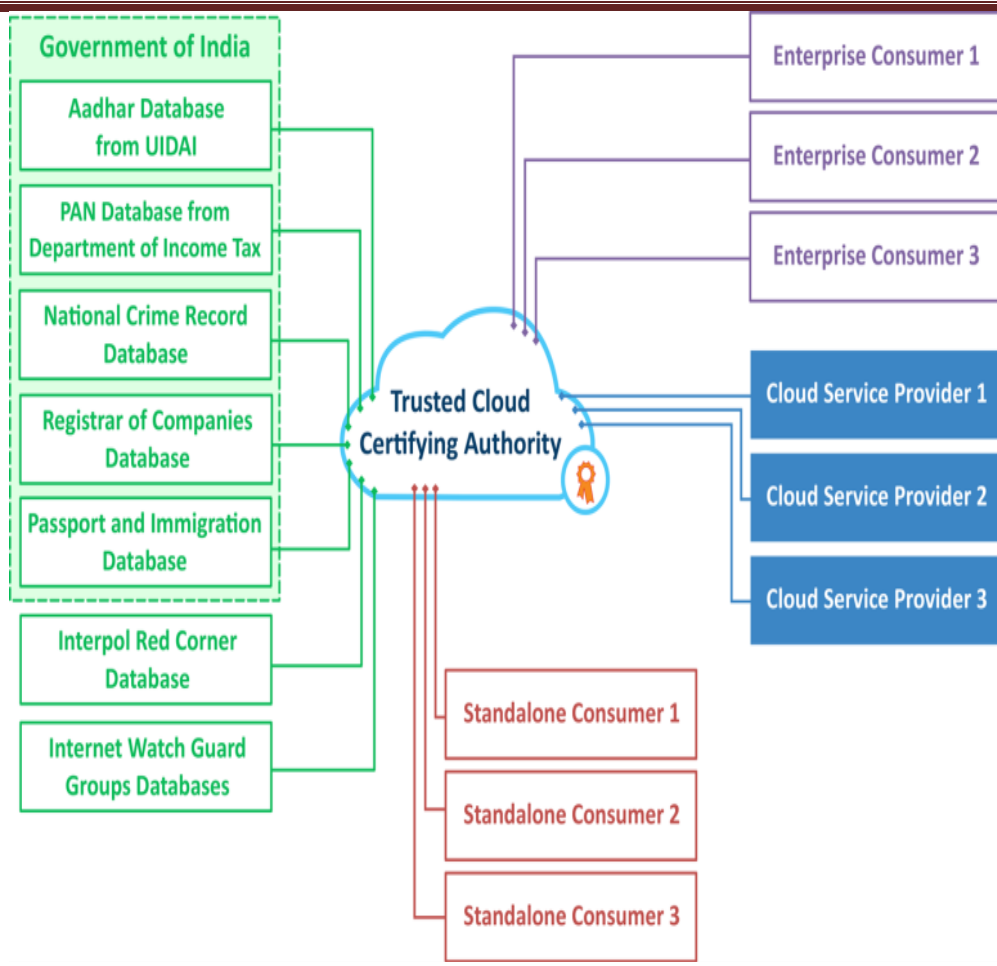

Figure.2 Architecture for the proposed model-Trusted Cloud Certifying Authority

The figure.2 indicates the proposed architecture model for Trusted Cloud Certifying Authority (TCCA).The key parameter will be used to construct the cloud trust model Framework to provide confidentiality, integrity, identity management, privacy, reputation and availability. The trust scoring will be on positive scale and for any negative transactions the rating will undergo a negative adjustment. This scoring will be dynamic and will be managed by TCCA. The TCCA will be calculating the trust score on a real time basis without recreating a duplicate data base of its source data. At any point in time, the TCCA will not store any data. TCCA will be running only the algorithm and publishes the score real time using its front-end server accessible by authorised cloud service providers or consumers. The cloud service provider at present does not know any back ground of its current consumers. In this case, once the TCCA publishes the trust score, cloud service provider can state that only the consumers (let it be enterprise or standalone) who has a trust score of "X" and above will be provisioned in its cloud services .Similarly, consumers can state that any cloud service provider who has the trust Score of "X" and above can only respond to its Request for Proposal (RFP) or it will contract .This trust model reduces the usage of cloud computing resources by the bad elements who uses cloud computing power to launch an attack.

4. Result and Discussion

The cloud service with the best trust score is chosen for recommendation, on the basis of security parameter.

The probability of the service 'S' recommended to the user 'U'. Pearson's correlation can be calculated using the following equation

$$\hat{R}_{U,S} = \frac{\sum_{U^* \in U} Sim_{U,U^*} R_{U^*,S}}{\sum_{U^* \in U} Sim_{U,U^*}} \quad \text{.....(1)}$$

Where,$R_{U^*,S}$is the estimated value and sim_{U,U^*} denotes the preference similarity of the users 'U' and 'U*'. It is calculated by using the following formula:

$$Sim_{U,U^*} = \frac{\sum_{S \in C_S}(r_{U^*,S} - \overline{r_U^*})(r_{U,S} - \overline{r_U})}{\sqrt{\sum_{S \in C_S}(r_{U^*,S} - \overline{r_U^*})^2}\sqrt{\sum_{S \in C_S}(r_{U,S} - \overline{r_U})^2}} \quad \text{.....(2)}$$

Where$r_{U*,S}$is the rating given to the cloud service 'S' by the user 'U∗', $S \in C_S$is the cloud service rated by the users 'U' and 'U∗', $r_{\bar{U}}$and$r_{\bar{U*}}$ are the average rating values of the users.

In order to accomplish the predictive rating score of the cloud user on the basis of probability of service recommended to the user. Finally, the prediction phase generates the results according to the similarity measure and user preferences. The decisions are made using the user profiles constructed in the information gathering phase, which is used as a training set in the learning phase.

4.1 Trust authority module

The cloud service provider consists of various attributes but it can be validated and ranked based on the respective parameters like confidentiality, identity, management, reliability, reputation, privacy. These attribute scores are used to calculate the trust result and rating with the help of collaborative filtering algorithm. The cloud service provider rank is predicted by the rating score of the cloud user on the basis of the feedback.

Table.1 Rating of the best Cloud Service

Service Name	Confidentiality	Reliability	Identity	Management	Privacy	Reputation	Trust Result	Rating	Rank
CSP 4	0	54.5	54.5	0.0	51.5	0.0	54.0	4.91	1
CSP 5	250	308.0	248.0	0.0	319.0	312.0	31.0	4.61	2
CSP 3	9	9.0	10.0	0.0	8.0	10.0	9.0	4.50	3
CSP 1	3393	3765.0	0.0	3369.0	3941.0	3657.0	3855.8	4.25	4
CSP 6	0	19.0	0.0	0.0	18.0	18.0	16.0	4.00	5
CSP 2	277	270.0	0.0	0.0	358.0	0.0	317.5	3.24	6

Table.1 shows the best cloud service name. cloud name = CSP4 technical services, trust result rating = 4.91 and rank is 1.

4.2 Comparison based on cloud rating

The trust score will be published by the cloud trust authority which can be accessed by either the cloud service provider or the consumer. The comparison of cloud services rating or ranking based on trust score is evaluated and shown in figure.3

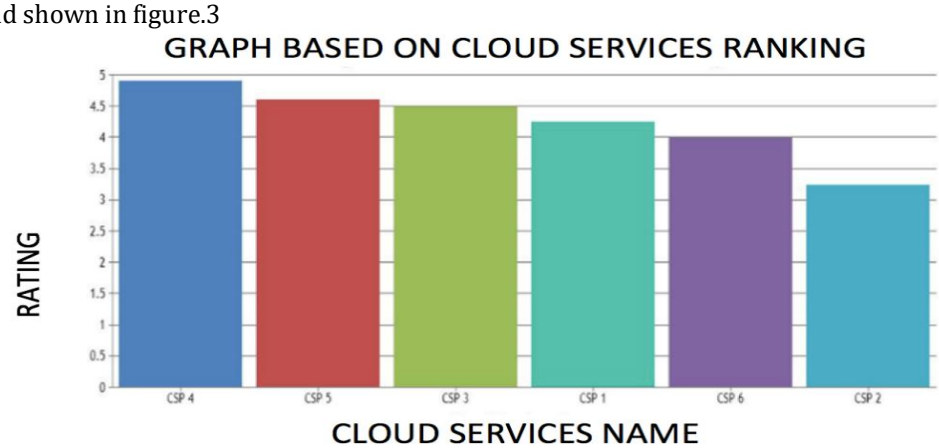

Figure.3 Graph based cloud service rating

4.3 Comparison for Trusted and Untrusted Consumers

The comparison of trusted and untrusted consumer for enterprises and individuals are evaluated and shown in figure.4.The trust result of consumers has various attributes namely, financial stability, legal regulatory issues, security incident, criminal background and history of complaints. Therefore the feedback of the consumer is used as a key role to identify the input of the above mentioned attributes. To evaluate the trust result as trusted and untrusted consumer for both enterprises and individuals by use of collaborative filtering algorithm. This trust results for both enterprises and individuals are managed by the Trusted Cloud Certifying Authority (TCCA).

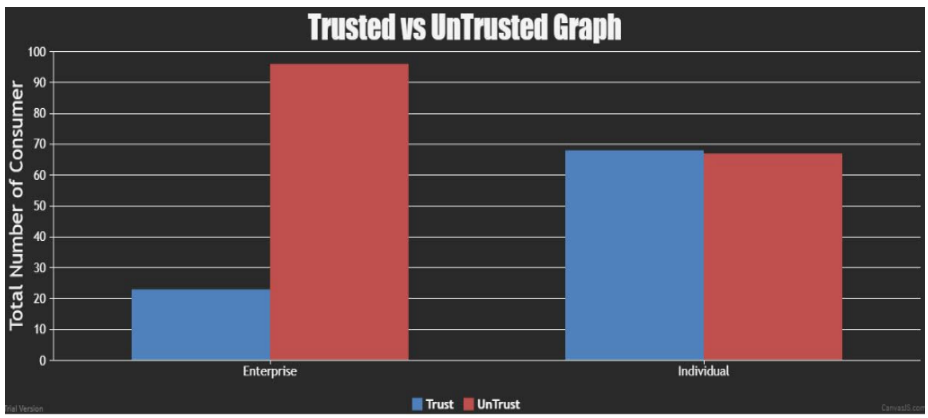

Figure.4 comparison of Trusted and Untrusted cloud service provider

5. Conclusion

The proposed trust authority models reduced the bad elements using the cloud services and also prevent unethical cloud service providers to offer a service with the help of ranking based on trust score. This scoring will be dynamic and will be managed by the Trusted Cloud Certifying Authority (TCCA). The dynamic continuous evaluation of both cloud service providers as well as the consumers helps to identify the rogue elements and prevent the unscrupulous elements from offering as well as using the services. There are several cases wherein the cyber criminals are using the free computing resources to launch attack on a destined target and cause significant damage. This model is expected to bring down the number of usage of free cloud based computing power by cyber criminals. These categories include trust models that ensure the availability, integrity and confidentiality of data on cloud by using certificates from standardized body. Thus the data can be securely shared with the authorized users by adopting the collaborative filtering techniques.

Reference

1. Rizwana Shaikh and Dr. M. Sasikumar, "Trust Model for Measuring Security Strength of Cloud Computing Service", Elsevier B.V, International conference on Advanced Computing Technologies and Applications (ICACTA), 2015.
2. Usvir Kaur and Dheerendra, "Trust: Models and Architecture in Cloud computing",International Journal of Computer Science and Information Security (IJCSIS), Vol. 13, No. 12, December 2015.
3. K. Gokulnath and RhymendUthariaraj, "A Survey on Trust Models in Cloud Computing", Indian Journal of Science and Technology, Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/108685, December 2016.
4. Zhu C, Nicanfar H, Leung VC, Yang LT. An authenticated trust and reputation calculation and management system for cloud and sensor networks integration. IEEE Transactions on Information Forensics and Security. 2015 Jan; 10(1):118–31.
5. A.Logeshwari, M.Aiswariya, V. Swathi and K.Vivekavarthini, "Data Security, Privacy, Availability And Integrity In Cloud Computing: Issues And Solution", International Journal of Computer Science and Mobile Applications, Vol.6 Issue. 2, February- 2018, pg. 82-89 ISSN: 2321-8363.
6. Siani Pearson, "Privacy, Security and Trust in Cloud Computing", Springer, 2012.
7. AnupamDas,MohammadMahfuzul Islam, "Securedtrust: A Dynamic Trust Computation Model For Secured Communication In MultiagentSystems",IEEE Transactions on Dependable and Secure Computing, Volume: 9, Issue: 2, March-April 2012).
8. Zheng Yan and Christian Prehofer, "Autonomic Trust Management for a Component-Based Software System" ,IEEE Transactions on Dependable and Secure Computing (Volume: 8, Issue: 6, Nov.-Dec. 2011.
9. Noor T, Sheng Q, Yao L, Dustdar S &Ngu A 2015, 'CloudArmor: Supporting reputation-based trust management for cloud services', IEEE Transactions on Parallel and Distributed Systems.

10. Amor.Wang S, Sun L, Sun Q, Wei J & Yang F 2015, 'Reputation measurement of cloud services based on unstable feedback ratings', International Journal of Web and Grid Services, vol. 11, no. 4, pp. 362 - 376.
11. Li W, Ping L, Qiu Q & Zhang Q 2012, 'Research on trust management strategies in cloud computing environment', Journal of Computational Information Systems, vol. 8, no. 4, pp. 1757-1763.
12. Sultan Aldossary and William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016.
13. Banirostam H, Hedayati A, Zadeh AK &Shamsinezhad E 2013, 'A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure', 15th International Conference on Computer Modelling and Simulation (UKSim), 2013 UKSim pp. 717-721.
14. Shaikh R &Sasikumar M 2015, 'Trust Model for Measuring Security Strength of Cloud Computing Service', Procedia Computer Science, vol. 45, pp. 380-389.
15. Sidhu J & Singh S 2014, Peers feedback and compliance based trust computation for cloud computing, in Security in Computing and Communications, Springer, pp. 68-80.
16. Habib SM, Varadharajan V &Muhlhauser M 2013, 'A trust-aware framework for evaluating security controls of service providers in cloud marketplaces', 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2013, pp. 459-468.
17. Fan W-J, Yang S-L, Perros H & Pei J 2015, 'A multi-dimensional trust-aware cloud service selection mechanism based on evidential reasoning approach', International Journal of Automation and Computing, vol. 12, no. 2, pp. 208-219.
18. Abbadi IM &Alawneh M 2012, 'A framework for establishing trust in the Cloud', Computers & Electrical Engineering, vol. 38, no. 5, pp. 1073-1087.