Institute of Industrial and Computer Management and Research, Nigdi, Pune

MCA-1 (Sem II)

(2022-2023)

Fuzzy Authorization on Cloud Computing By Using Merging Technique

Nitesh Shankar Rai

Institute of Industrial and Computer Management and Research, Nigdi, Pune

46rai.nitesh@gmail.com

8788247009

Nitin Sanjay Bhopale

Institute of Industrial and Computer Management and Research, Nigdi, Pune

nitinbhopale53@gmail.com

9168348200

Prajwal Rameshwar Kute

Institute of Industrial and Computer Management and Research, Nigdi, Pune

prajwalkute999@gmail.com
8552947782

Fuzzy Authorization on Cloud Computing By Using Merging Technique

Abstract-

Despite the growing deployment of mission critical applications on computing systems, trust and security continues to hinder its full adoption and deployment on cloud computing platforms. In addition to accountability and non-repudiation on the cloud deployment, end-users want to be confident of availability and reliability of services. For any cloud platform to be secure and trusted, the individual layers of the platform must be secure as there is no 'one fits all solution' for securing all the layers. This work presents a multi-layer trust security model (MLTSM) based on unified cloud platform trust that employs a fuzzy logic combination of on-demand states of several different security mechanisms, such as identification, direct and in-direct trust, across all cloud layers. In addition, results from a MATLAB-based simulation of the model are also presented. A MLTSM can improve the secure deployment of cloud infrastructure in mission critical sectors such as electrical power system operation, as it provides empirical evidence that allows direct (on-demand) determination and verification of the trust state of any given cloud computing platform or service. Such a modelling approach is useful for comparison,

classification and improving end-user confidence in selecting or consuming cloud computing resources.

KEYWORDS- Genetic Algorithm, Virtual Machine migration, Bandwidth utilization

I. INTRODUCTION

In recent years, cloud computing has attracted the attention of many researchers around the world, and various programs, infrastructures, and frameworks have been created for it by several companies in the world [1–4]. In fact, cloud computing, as a new technology, provides a fully scalable, accessible, and flexible computing platform for a variety of applications [5]. Due to the various applications that cloud computing has found in various aspects of life, the issue of providing security in cloud computing communications and data stored in it, has been considered by users and providers of cloud computing services. According to some research conducted at Berkeley University, trust management and security optimization have been identified as the most important issues in using various cloud computing services [3, 6–8]. Cloud computing due to its distributive nature, very dynamic space, and lack of transparency in performing cloud computing faces many challenges in providing security and gaining trust. In order to improve security in performing cloud computing, trust management can play a very effective role [9, 10]. (is article is organized into five sections. In the second part, we examine some of the related work done by various researchers. In the third section, we present a new framework for trust management in multicloud environments. In the fourth section, we bring the simulation results of the

framework presented in this research, and finally, in the fifth section, we will conclude.

II. Related Work

level of trust and confidence in cloud service providers is one of the important parameters to provide a reliable service for the cloud service user. Liu and colleagues [11] proposed a method in which reliable cloud service providers for SaaS applications were selected based on their credibility and trust [12]. Many of the proposed models for measuring trust are based on records of trust in various cloud service providers [13, 14]. Accordingly, these models can be divided into two general categories, which are subjective and objective trust models [15]. To measure the level of objective trust, parameters related to the quality of service (QoS) delivery are used. Fan and colleagues [16] proposed a concept called "objective trust" for software agents. (e researchers explained the trust between agents based on real-life experiences. Lin et al. [17] proposed a new framework for MANET networks in which one node evaluates the reliability of another node using direct observations. To calculate the level of trust in the subjective method, we can use the amount of feedback received from users using various cloud services [16]. Uikey et al. [18] proposed a new trust management model in which all information about different cloud service providers and the level of trust is recorded and stored. In this study, SLA models were used to calculate the reliability of cloud service providers. Alhamad et al. [3] proposed a new SLA-based trust management model to predict the level of trust in cloud service providers. In the proposed model, SLA-based conceptual framework is integrated with a trust value

management. Chakraborty et al. [19] applied the parameters extracted using the SLA to measure the reliability of cloud services. Some of the most commonly used SLA-based models are probability-based trust model, intuitive reasoning-based trust model [20], Bayesian-based trust model, Dempster–Shafer model, Fuzzy logic-based trust [21], cloud computing trust model [22], and so on. Siadat et al. [23] proposed a new model for managing trust in cloud computing that uses game theory to detect fake feedback [24]. Chen et al. [25] proposed a new trust management model for the Internet of (ings (IoT) in which trust management at different levels of the IoT was examined. In the study by Guo et al. [26], a new model for managing trust in the IoT suggests that methods for assessing trust are examined based on five common design dimensions (including trust composition, dissemination, aggregation, updating, and shaping). Din et al. [27] examined trust management methods without performing any classification. Various studies have been conducted to combine methods of objective and subjective trust. Yuan et al. [28] proposed a framework for assessing trust that uses a combination of objective and subjective trust methods that calculate and rate trust based on a combination of users' trust and credibility. Ngo et al. [29] examined the relationship between the level of objective trust and subjective trust and expressed the characteristics of each of these two types of trust. Sangaiah et al. [30] with using machine-learning techniques proposed a new method to maintain the confidentiality of the geographical location of PBS portable users. (e proposed method had three phases. During these phases, using the integration of decision tree techniques and the nearest neighbor, the user's geographical location was determined, and using the sequence of routes transferred and using hidden Markov models, the user's destination was identified. Along with maintaining the confidentiality of users' position, these researchers showed

that the accuracy of this method in establishing position in PBS was equal to 90%. (e results of the implementation of the proposed method by these researchers showed that the accuracy of this method in establishing position confidentiality in PBS was equal to 90%. Sangaiah et al. [31] defined a weight called relay ability for each node according to the sensor network topology. (ese weights are calculated by the head and reported to all sensor nodes. When a target enters the area covered by sensor nodes, a signal is sent to CH via a path that has a predefined maximum weight in the network. (e simulation of the proposed method in this research showed that this method has better results than other tracking methods based on the criteria of network power consumption, power consumption and power for GRTT, dynamic energy efficient 2 Mathematical Problems in Engineering routing (DEER) protocol, and virtual power-based energy consumption (VFEM). In the study by Sangaiah et al. [32], an energy-aware green adversary model has been proposed for use in intelligent industrial environments by achieving confidentiality. In this study, researchers explored various aspects of preserving geographic location information and information confidentiality. Finally, we proposed a new model which has the capacity to make prediction based on a schedule in real-time situations, it can make connections, respond to user demands, and minimize energy consumption. (e experimental results of these researchers showed that their proposed model can be five times more energy saving compared with other methods. Mousa et al. [33] used a trust model based on the fuzzy logic system to evaluate trust values. (ey proposed a new method for this purpose, which gives cloud users the ability to assess the reliability of cloud service providers. Simulations of their proposed method showed that the accuracy of the evaluations performed by these researchers was higher compared with other works.

III. Our Proposed New Trust Management Framework in Multicloud Environments

We propose a new framework for trust management using cloud service providers (TSPs). We try to cover several problems that exist in the field of trust management in multicloud environments with this proposed framework. (e trust management framework proposed in this study is seen in Figure 1. CSPs (cloud service providers) are responsible for providing services to cloud service users. In cloud computing, a variety of services are provided to users by CSPs. (e most common types of services are SaaS, PaaS, and IaaS. CSPs also provide services to CSUs (cloud service users). CSUs send their requests to TSP (which is one of the CSPs). (e selection of this TSP among CSPs is done by different selection algorithms. (e main task of TSP is to select the appropriate CSP to receive and respond to requests sent from CSU. Another function of TSP is to verify CSP reliability. 3.1. SLA Monitor Agent. SLA monitor agent is located on CSUs side. It monitors services behavior and services performance that if CSUs meet SLA or not. SLA monitor agent collects data in the interaction between CSPs and CSUs and also its responses to control requests. A control request is sent by TSP. SLA monitor agent continuously collects control information from server side. Control information contains SLA performance parameters. 3.2. Monitoring Information Collection Agent. (e responsibility of monitoring information collection agent is collecting monitor agents information on SLA which has an agreement with TSP. Collected information by this agent is applied to evaluate objective trust values. (e following information is maintained by the monitoring information collection agent: (i) CSPs list is monitored by TSP (ii) SLA monitoring information received from SLA monitor agent that is in agreement with TSP Before receiving the CSUs service from the CSPs, an SLA

contract is agreed between them with various parameters. (is SLA contract is the output of the SLA negotiation component, which determines the level of service that the CSUs and CSPs agree on. Some of the parameters in the SLA are availability, response time, and so on, which are agreed upon, based on which the server agreements that are closest to the CSUs request are selected in the next steps.

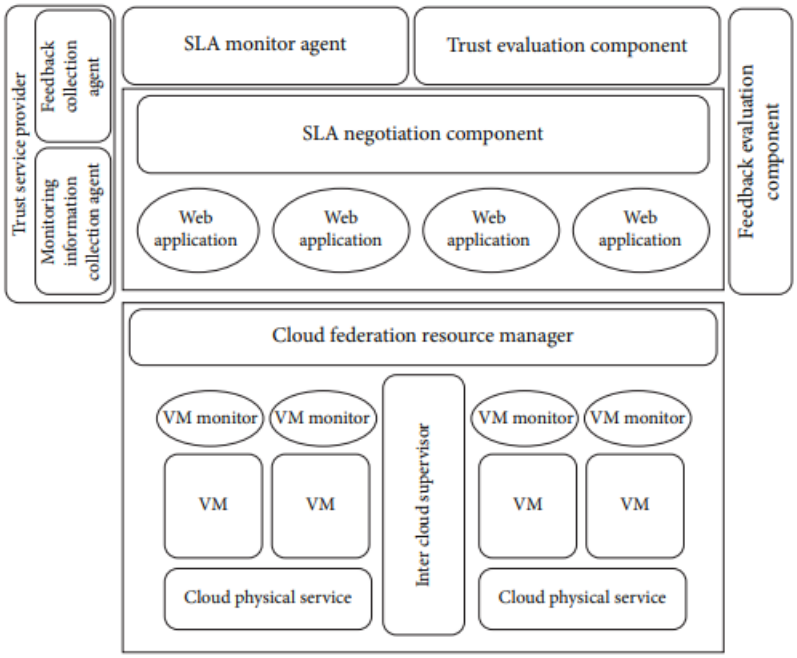

FIGURE 1: Our proposed trust management framework in multicloud environments.

CONCLUSION

In this paper, a new trust management framework for multicloud environments has been proposed. (e advantages of this framework are as follows: (i) Subjective trust value and objective trust value applied to calculate trust values. (ii) Objective trust value and subjective trust value are multidimensional parameters. (iii) Feedback evaluation component was applied in this framework. (e Feedback

evaluation component task is identifying and rectifying fake feedbacks that any framework does not apply to this component yet. Simulation results had shown the performance of this component, and it shows the effect of this component on trust values. (iv) Trust negotiation component has used the platform that the output of its component is SLA contract.

One agent of the SLA negotiation component is the demand trust evaluation component. (is component selects the CSPs that have the nearest adoption with CSU request, and finally this component causes increase in the service satisfaction and trust values average. (e simulation results confirm it. (v) (e proposed framework increased trust values rather than other models (SLA-based model, feedback-based model, and multicloud model). As future work, the trust management model can be proposed along with the detection of fake feedback in other applications such as fog computing and the Internet of (ings. In the case of failures, it can be noted that if several cloud service users colluded with each other and attacked a cloud service provider for a period of time, the proposed feedback evaluation component cannot detect fake feedback from other feedbacks. As a future work, it is planned to introduce a trust management model with the feature of detecting fake feedback in IoT networks and fog computing. Game theory can also be used to detect fake feedback in the feedback evaluation component of trust management models

REFERENCES:

[1] N. Jafari Navimipour, A. M. Rahmani, A. Habibizad Navin, and M. Hosseinzadeh, “Expert cloud: a cloud-based

framework to share the knowledge and skills of human resources," Computers in Human Behavior, vol. 46, pp. 57–74, 2015.
[2] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: vision, hype, and reality for delivering it services as computing utilities," in Proceedings of the 2008 10th IEEE International Conference on High Performance Computing and Communications, Dalian, China, September 2008.
[3] M. Armbrust, A. Fox, R. Griffith et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
[4] N. Jafari Navimipour, A. Masoud Rahmani, A. Habibizad Navin, and M. Hosseinzadeh, "Resource discovery mechanisms in grid systems: a survey," Journal of Network and Computer Applications, vol. 41, pp. 389–410, 2014.
[5] R. Buyya, R. Ranjan, and R. N. Calheiros, "Intercloud: Utilityoriented federation of cloud computing environments for scaling of application services," in Proceedings of the International Conference on Algorithms and Architectures for Parallel Processing, Busan, Korea, May 2010.
[6] P. Xiao, Z.-G. Hu, and Y.-P. Zhang, "An energy-aware heuristic scheduling for data-intensive workflows in virtualized datacenters," Journal of Computer Science and Technology, vol. 28, no. 6, pp. 948–961, 2013.
[7] T. H. Noor and Q. Z. Sheng, "Trust as a service: a framework for trust management in cloud environments," in Proceedings of the International Conference on Web Information Systems Engineering, Sydney, NSW, Australia, October 2011.
[8] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in Proceedings of the 2010 IEEE Second International Conference on Cloud Computing Technology and Science, Indianapolis, IN, USA, November 2010.

[9] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. In´acio, “Security issues in cloud environments: a survey,” International Journal of Information Security, vol. 13, no. 2, pp. 113–170, 2014.
[10] I. M. Abbadi, “A framework for establishing trust in Cloud provenance,” International Journal of Information Security, vol. 12, no. 2, pp. 111–128, 2013.
[11] C. Tang and J. Liu, “Selecting a trusted cloud service provider for your SaaS program,” Computers & Security, vol. 50, pp. 60–73, 2015.
[12] I. M. Abbadi and A. Martin, “Trust in the cloud,” Information Security Technical Report, vol. 16, no. 3-4, pp. 108–114, 2011.
[13] I. U. Haq, I. Brandic, and E. Schikuta, “Sla validation in layered cloud infrastructures,” in Proceedings of the International Workshop on Grid Economics and Business Models, Ischia, Italy, August 2010.
[14] W. Conner, “A trust management framework for serviceoriented environments,” in Proceedings of the 18th International Conference on World Wide Web, Madrid, Spain, April 2009.
[15] Z. Malik and A. Bouguettaya, “Rateweb: reputation assessment for trust establishment among web services,” =e VLDB Journal, vol. 18, no. 4, pp. 885–911, 2009. [16] W. Fan, S. Yang, and J. Pei, “A novel two-stage model for cloud service trustworthiness evaluation,” Expert Systems, vol. 31, no. 2, pp. 136–153, 2014.
[17] J. Y.-j. Hsu, K.-J. Lin, T.-H. Chang, C.-j. Ho, H.-S. Huang, and W.-r. Jih, “Parameter learning of personalized trust models in broker-based distributed trust management,” Information Systems Frontiers, vol. 8, no. 4, pp. 321–333, 2006.
[18] C. Uikey and D. Bhilare, “A broker based trust model for cloud computing environment,” International Journal of

Emerging Technology and Advanced Engineering, vol. 3, no. 11, pp. 247–252, 2013.
[19] S. Chakraborty and K. Roy, “An SLA-based framework for estimating trustworthiness of a cloud,” in Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, June 2012.
[20] W. Fan and H. Perros, “A novel trust management framework for multi-cloud environments based on trust service providers,” Knowledge-Based Systems, vol. 70, pp. 392–406, 2014.