RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

A Trust-based framework for the assessment of security in cloud computing environment

[1*]Anand Kumar Mishra, [2]Mayur Rahul, C.S. Raghuvanshi[1]

[1]Faculty of Engineering & Technology, Rama University Uttar Pradesh, Kanpur
[2]UIET, Chhatrapati Shahuji Maharaj University Uttar Pradesh, Kanpur

Abstract: The cloud computing is very critical and important part in today's competitive market. The different services of cloud computing has been available in the market so far. The framework available for the service providers is different in their nature. It is a great challenge to evaluate the services of each and every cloud service provider. So, the objective of the research is to propose a framework which is capable evaluating security of cloud environment based on trust. The model is used to examine the security strength and give some trust value for the given parameters. They are also used to evaluate the security and validation of the given model. The suitableness of the framework is also justified by trust score of given cloud services. This framework acts as a ranking system and threshold for evaluating the security of the cloud environment.

Keywords: Cloud computing; Cloud Computing Security; Security and Privacy; Trust Model; Mobile Agent; Trust; cloud service provider.

1.Introduction: Cloud computing has become a well-known prototype of service delivery and computing. Though, one common question arise in the mind of potential user of cloud services that "can I calculate the trust score of the given cloud services?". Further, what is the exact meaning of "trust" with respect to cloud computing? and what is the foundation of that trust?. If the properties of the given cloud are used to calculate the trust score, then on what criteria the users believe in the properties given by the cloud providers?. Who takes the responsibilities for monitoring the evaluation, assessing, measuring and validating the cloud properties. The answers for these questions are very important because of the wide application of cloud environment and also for the trust based evaluation of cloud service providers. As described by Michael et al.[1] "thegrowing importance of cloud computingmakes it increasinglyimperative that we grapple with the meaning of trustin the cloud and how the customer, provider, and societyin general establish that trust."

The challenges and issues in trust score in cloud computing have been discussed with respect to different approach[2,3]. Differenttools and models have been introduced [4,5]. Every paper gives the limited view of cloud trust, but lack of describing entire picture that how properties are combined to form a system which is perfectly grounded in trust, used to give trusted framework to trusted cloud services. According To NIST cloud computing architecture for reference states that recognize the cloud auditors and brokers as entities responsible for the smooth conduct of evaluation of cloud services. Although, there are lot of research found in

trust analysis and trust have been made between end users and cloud services with the help of these properties (fig. 1).

Security is another important concern in cloud computing environment. Cloud service security is basically concern with the terms like authorization, authentication, data protection etc. These are the basic objectives of the security of cloud computing and very important when going towards security of cloud. Hence, a framework which is used to evaluate and assess the performance of the security strength is required in real world. The primary job of the research is to propose a framework which is capable of calculating the security strength of the cloud. It basically consists of trust score which represents the entire security strength of the cloud. The calculation of trust score can be achieved by various parameters associated with the cloud service. A trust oriented framework is used to calculate the trust score. Various entities are identified to calculate the score. Hence, this trust framework can be used to evaluate the strength and ranking system of the different service providers (fig. 2).

Because of the complex nature of various cloud services, many cloud users can't take decisions to applying a cloud service based on trust technique. These decisions are mainly based on these trust technique and properties, which are more accurate, more responsible, and more stable. We are going to propose a framework to calculate the trust score with the help of various properties found in cloud computing environment.The main findings of this paper are as follows

(1) We investigate the trust technique in cloud computing.
(2) We propose the society based trust technique for evaluation of security services of cloud.
(3) We introduce different properties of cloud to calculate the trust score.
(4) We apply trust score mechanism in different existing service providers.

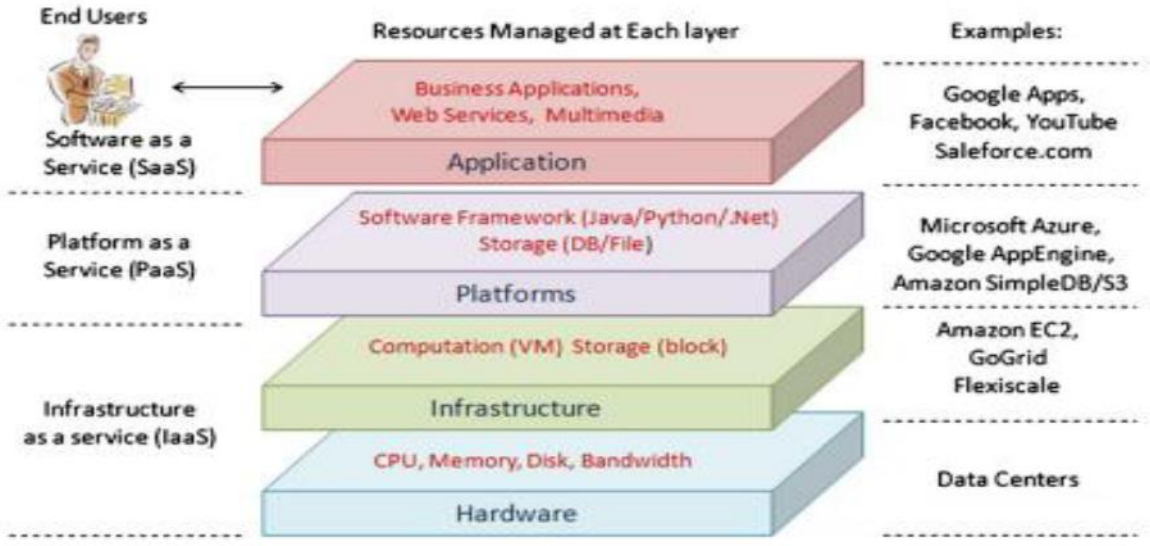

Figure 1: Cloud computing architecture

This paper is summarized as follows: (1) we define the cloud computing and trust based technique. (2) we review the state-of-the-art of cloud computing and different trust based model. (3) we discuss various properties to calculate the trust score. (4) we present an desegregated view of the trust technique for cloud environment,and analyse the trust connecting cloud entities. (5) Finally, we give a conclusion and identify future research.

(2) Related Works: During the past decade many researchers used trust model in their work. These trust models are used to protect computer and network that can be also applied in cloud computing environment.

Shantanu et al. introduced a 2-tier framework depends on collaborative agent and trust model to prevent cloud resources by observing unauthorised access [6]. They are able to introduce trust model based on trustworthiness of system by evaluating updated and current trust degree. The trust degree is calculated for service provider of the domain and service request. The used the proxy server as a communication medium between domains and also for the authentication of every service model.

Florina et al. introduced a framework based on trust model for the security of cloud computing environment [7]. The used the concept of two level for cloud users and cloud providers. They also used double agents to evaluate and update the trust degree factor for the domain and user using some trust function. They were also able to maintain the user activities and their database. Further, the trust degree of users greater than the particular threshold trust score only can access and able to get the relevant information from cloud provider. They are also able to identify the malicious access user and also able to remove that user from its domain.

Figure 2: Cloud security requirement

The major ascendancy of this model is that the domain is unaffected by nontrusted users. This model also has some disadvantage. It increases the workload of domain and also unable to protect from malicious activities without service provider information of user activity.The

proxy server used for the communication is also very weak because if there is some problem in servers then end users unable to communicate with the service provider.

Priyank et al. introduced a trust score based model for cloud computing architecture [8]. Different mobile agents have been kept as a security agent to keep track of all information needed from virtual machines. This information is very useful in monitoring of unauthorised access of data and virtual machines. These agents are also used to keep track of integrity and authenticity of virtual machines. These agents are able to migrate and circulate in the network,perform and replicate the assigning tasks to keep track of virtual machines. These agents can be used as a monitoring agent in different levels of cloud infrastructure in order to keep track of threats and resource utilization. Further, they are also used to produce a strong trust between the end users and service providers of the cloud. Their framework is unable to identify the importance of identity management, user identification and agents security.

Amir et al. introduced the framework to overcome the problem of security in cloud data storage [9]. Their framework is also able to verify the data availability and security in cloud computing environment based on multi agent system model. The proposed framework comprise of two layers: cloud data storage layer and agent layer. Their framework was based on six agents. Every layer has some specific task. The specific tasks are: User assistance in operating, a collective interface; indulge different failures in distributed systems, allow the user to rebuildthe initial data by downloading the vectors fromthe servers, storing system information and associated information, as well as storing the data and messages shared betweenvarious agents.

(3) Proposed Methodology: Calculating trust values in a cloud environment involves assessing various factors related to the reliability, security, and performance of the cloud services and providers. While there isn't a one-size-fits-all formula for calculating trust values, you can consider the following general steps and factors:

1. **Define Trust Criteria**: Identify the specific criteria or attributes that contribute to trustworthiness in the cloud environment. These criteria may include security measures, reliability, performance, compliance with regulations, transparency, customer satisfaction, and reputation.

2. **Assign Weights to Criteria**: Assign weights to each trust criterion based on its importance or priority in your evaluation. For example, security and reliability may be weighted more heavily than other factors.

3. **Collect Data**: Gather relevant data and information to assess each trust criterion. This may involve reviewing security certifications, SLAs, performance metrics, customer reviews, audit reports, and any other relevant documentation.

4. **Normalize Data**: Normalize the data to ensure that all metrics are on the same scale for comparison purposes. This may involve converting data into a common unit or percentage format.

5. **Calculate Trust Score**: Calculate a trust score for each cloud service or provider based on the weighted average of the normalized values for each criterion. This can be done using a weighted sum or another appropriate aggregation method.

6. **Adjust for Context**: Consider contextual factors that may impact trustworthiness, such as the specific requirements and preferences of your organization, the sensitivity of the data and workloads being hosted in the cloud, and the industry or regulatory standards that apply.

7. **Iterative Evaluation**: Periodically reassess trust values based on changes in the cloud environment, updates to security measures, performance improvements, or other relevant factors. Continuous monitoring and evaluation are essential for maintaining trust in the dynamic cloud landscape.

8. **Feedback Mechanism**: Incorporate feedback from users, stakeholders, and industry experts to validate and refine the trust calculation methodology. User experiences and perceptions can provide valuable insights into the trustworthiness of cloud services and providers.

4. Experiment and results:

a. Define Trust Criteria:

- Criteria: Security, reliability, performance, compliance, customer satisfaction.
- Weights: Assigned based on importance, e.g., security (30%), reliability (25%), performance (20%), compliance (15%), customer satisfaction (10%).

b. **Data Normalization**:

- Convert data into a common scale or format for comparability.
- Normalize metrics (e.g., uptime percentage, response time) to a range between 0 and 1.

c. **Calculating Trust Scores**:

- Weighted Average Method: $TrustScore=(W1\times C1)+(W2\times C2)+\ldots+(Wn\times Cn)TrustScore=(W1\times C1)+(W2\times C2)+\ldots+(Wn\times Cn)$
- Where $WiWi$ is the weight assigned to criterion ii and $CiCi$ is the normalized value of criterion ii.

Experimental Execution:

- Collect and organize data from various sources.
- Normalize data and assign weights to criteria.

- Calculate trust scores for each CSP using the defined methodology.

CSP	Security	Reliability	Performance	Compliance	Customer Satisfaction	Trust Score
CSP A	0.85	0.90	0.85	0.80	0.75	0.843
CSP B	0.90	0.85	0.80	0.85	0.80	0.837
CSP C	0.80	0.80	0.90	0.75	0.85	0.826
...	...	...	...	...	...	...

Analysis of Results:

- CSP A has the highest overall trust score, primarily due to its strong security and reliability measures.
- CSP B performs well in compliance and customer satisfaction, but slightly lower in reliability and performance.
- CSP C excels in performance but falls short in compliance and security.
- Variations in trust scores reflect differences in strengths and weaknesses among CSPs, providing insights for decision-making.

5.Discussion and Conclusion:

a. Trust scores provide a quantitative basis for evaluating and comparing CSPs in the cloud environment.

b. Strengths and weaknesses identified through the analysis can guide decision-making regarding CSP selection and risk management strategies.

c. Limitations such as data availability, subjective weighting, and evolving security threats should be considered in interpreting the results.

References:

[1] Michael B (2009) In clouds shall we trust? IEEE Security and Privacy 7(5):3–3. http://dx.doi.org/10.1109/MSP.2009.124

[2] Everett C (2009) Cloud computing: A question of trust. Computer FraudSecurity 2009(6): 5–7. http://dx.doi.org/10.1016/S1361-3723(09)70071-5

[3] Garrison G, Kim S, Wakefield RL (2012) Success factors for deploying cloudcomputing. Commun ACM 55(9): 62–68. http://doi.acm.org/10.1145/2330667.2330685

[4] Abawajy J (2011) Establishing trust in hybrid cloud computingenvironments. In: Proceedings of the 2011 IEEE 10th InternationalConference on Trust, Security and Privacy in Computing andCommunications,.IEEE Computer Society, Washington, DC, USA.TRUSTCOM ’11, pp 118–125. doi:10.1109/TrustCom.2011.18. http://dx.doi.org/10.1109/TrustCom.2011.18

[5] Haq IU, Alnemr R, Paschke A, Schikuta E, Boley H, Meinel C (2010)Distributed trust management for validating sla choreographies. In:Wieder P, Yahyapour R, Ziegler W (eds). Grids and service-orientedarchitectures for service level agreements. Springer,US. pp 45–55. http://dx.doi.org/10.1007/978-1-4419-7320-7_5

[6] Shantanu Pal, SunirmalKhatua, NabenduChaki, SugataSanyal;"A New Trusted and Collaborative Agent Based Approach forEnsuring Cloud Security"; Annals of Faculty EngineeringHunedoara International Journal of Engineering; Vol. 10, Issue1, February, 2012. pp. 71-78. ISSN: 1584-2665.

[7] FlorinaAlmen´arez, Andr´esMar´ın, Celeste Campo and Carlos, “PTM: A Pervasive Trust Management Model for Dynamic Open Environments”, Proceedings of First Workshop on Pervasive Security, Privacy and Trust PSPT’04, Boston, USA, 2004.

[8] Priyank.s, Ranjita.s, Mukul.s, Security Agents: A Mobile Agentbased Trust Model for Cloud Computing, International Journal ofComputer Applications (0975 – 8887) Volume 36– No.12,December 2011

[9] Amir Mohamed, Rodziah A, Rusli Abdullah and Masrah M, Aframework of multi agent system to facilitate security of clouddata storage, Annual International Conference on CloudComputing and Virtualization, 2010.

[10] Alwesabi, A., &Okba, K. (2014). Security Method: CloudComputing Approach Based on MobileAgents. International Journal of New ComputerArchitectures and their Applications (IJNCAA), 4(1), 17-29.