Light Weight Trust Computing for Cloud Service Provider

Punithavalli V[1] , P.Sheela Gowr[2], M.Latha[3]
[1]Student, Department of Computer Science and Engineering,
Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamilnadu, India,
[2,3]Assistant Professor, Department of Computer Science and Engineering,
Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamilnadu, India,
[1]vpunithavalli27@gmail.com [2]sheela.se@velsuniv.ac.in [3]latha.se@velsuniv.ac.in

Abstract: Cloud computing is leading technology in the information technology industry. This is rapidly getting adapted from single user to enterprise applications. This majorly decreases the maintenance of infrastructure for everyone. Cloud Service is available as Saas, Paas and Iaas. This collectively provides different features to different user groups. Though cloud services are available in major variation, major concerns lies in security of the services and trustworthiness of cloud service providers. Cloud service trustworthiness is critical factor every cloud service provider and customer. Customer chooses most trusted cloud service provider and cloud service provider works to improve the trust factor so that it can increase the user base. This paper discusses different approach to traditional trustworthy cloud service provider. Adapted new lightweight probabilistic approach to improve performance of trustworthiness of cloud service provider. Additionally feedback mechanisms from various sources are used to improve the efficiency.

Keywords**:** *Trust Computing, Cloud, Broker, Secured cloud*

1. INTRODUCTION

In the past decade, cloud computing saw growth of multiple generations. Computing from physical to virtual model was implemented in this phase. Cloud technology improvised with virtual servers and data got placed in internet. Cloud technologies such as Iaas, Paas and Saas provided Infrastructure, Platform and Software showed different ways of application development and deployment to developers and end users. With multiple clouds collaborative environment possible currently major challenge lies in selecting appropriate cloud service provider. While selecting cloud service, since data needs to be saved in external environment, trust on cloud plays a very critical role.

End users select the most trusted cloud irrespective of features and cost. Hence every cloud service provider deploys various mechanisms to improve their trustworthiness.

In current world, light weight and fast trust computing are keys factors. This paper discusses various factor and methodologies involved in trust computing.

2. RELATED WORK

Author Malluhi and Khan has reviewed trust computing with perspective of what cloud user will expect in terms of security for their data and what cloud service provider will provide to satisfy customer needs. Their study revealed that for a cloud user major concerns for moving data cloud are ownership and control of data. Similarly they weight high on security and prevention. These parameters considered high for evaluating a cloud service provider. Less control and transparency will reduce the confidence of cloud user on service provider. Also studies revealed that certified service providers by certification authority on terms of transparency and security are more trusted by cloud user.

Singhal studied were towards cloud collaboration. This is in multiple cloud services will be used in collaborative fashion. For a user, they will be using a proxy layer were in background cloud will be collaborative approach. Author states that deep studies and testing is required to identify and security loop holes in these frameworks as multiple cloud player are involved.

Shen and Lieu proposed a new methodology for cloud collaboration. They proposed new methodology named harmony. This approach provided a integrated approach for resource and reputation management. This approach provides enhanced and efficient way of managing distributed resources. This methodology provides customer options to select resources based on the reputation. Cloud user has control to select resources based on reputation and hence this increases more transparency.

3. MATERIALS AND METHODS

Traditional trustworthy resource matching process is based on

- Monitoring large amount of data
- Trustworthy matching process

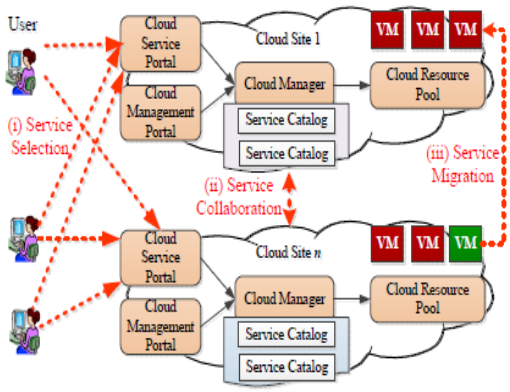


Fig.1: Cloud System

Traditional process involves deploying agents in all servers and this also creates higher overhead

Above Fig states challenges in current system as below parameters are not considered in current cloud systems.

Service Selection. Optimal cloud service should be selected and deployed.

Service Collaboration. Appropriated service components should be distributed in best collaborated approach.

Service Migration. Easy migration feature from one cloud service to different for optimal results.

Limitations

- Every instance requires an agent
- No feedback mechanism from other resources.
- CPU utilization will be drained for all resources.
- Less efficient

Proposed System

This paper proposes to use low overhead trust computing using fewer agents at broker end. This is to increase efficiency using feedback mechanism. i,.e To use agent at broker level and additionally add feedback mechanism from external sources.

- Feasibility and effectiveness is verified using performance analysis and experimental results
- Trusted cloud computing can be initialized to the cloud environment and to the actors involving in them.

- ✓ Less number of machine agents
- ✓ Feedback received from external resources
- ✓ More efficient in trust computing
- ✓ Machine CPU's will not be idle or wasted.

Detailed Design

In this design, machine agent segregated from application layer. Instead of adding machine agent in application layer, machine agent added in broker. Broker being the first entry point for all requests, it is decided to place the machine agent in broker.

This methodology is known as light weight probabilistic approach. This helps in looking for mal requests in earlier stage. This will improve security to application layer and in-turn improves the trust on cloud service providers for providing better cloud environment.

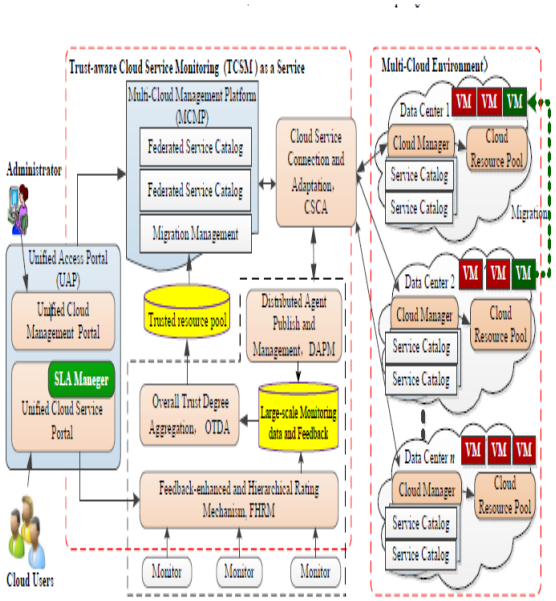


Fig.2: Architecture Diagram

Above is the architecture diagram of this proposed model. Model clearly depicts below

A) Unified Access Portal (UAP)

Unified access portal is web layer which provides user to select appropriated cloud service in multi cloud management platform. User will be provided and option to select the required trusted resource in this layer. Administer will maintain the virtual servers that provides as intermediary layer between users and providers.

B) Multiple Cloud Management Platforms (MCMP)

MCMP is federated service catalog. In this layer will have the details of available services and trust factor of all available services. This will automatically apply the highly trusted resources for user service request. Also the system provides feature for user to override the feature through manual selection.

a) Machine Agent in Broker

Opposed to traditional methodology, machine is placed in broker for quicker turn around.

b) Feedback Provider

This paper takes advantage of feedback providers in this model. Adding this in proposed model helps to improve system efficiency. External third party providers might also detect black listed and white listed users. Collecting this information will help in easily shortlist appropriate user requests. Keeping this list updated is a key factor to improve the trust.

c) Machine Agent

Machine Agent is the heart of the system. This validates the request from all sources. This does all below functionalities

- Payload validation
- Parameter validation
- SQL Injection
- Denial of Service
- White listed / Blacklisted IP

d) Payload validation

Payload is the content that reaches the broker before reaching the application. Attackers might create payload of different size or create payload to stall the application. This needs to be validated at broker end before reaching the application. Machine agent does this validating the payload size

e) Parameter validation

Once the payload is validated, parameters in payload should also be validated in order to avoid un-necessary processing of junk requests

f) SQL Injection

SQL Injection is one of way attackers use to collect data from application which is not efficiently coded. This way user can key in queries in application screen which can lead to disaster effect on application data. Adding security features in machine agent to avoid SQL Injection will help in greater security to the application. This adds more value to trust factor on application.

g) Denial of Service

Denial of Service is a major concern for applications. People can easily bring down the application instance by frequent requests to the application and also by manipulating large payload to the system. This Denial of Service will be identified by the machine agent deployed in broker. This adds up to score more value to trust agent.

h) White Listed / Black Listed

Feedback providers to easily collect the white listed and blacklisted users. This will help in avoiding un-necessary requests quickly. Along with this system will add up to the list the user list who is involved in above discussed scenarios

C) Implementation

A) Create cloud cluster environment

Cloud environment is created as the first step of this project. This is to get the environment setup with sample application and broker deployment. Later machine agent can be installed and trust of the cloud can be increased.

- Create AWS account
- Create EC2 instance
- Create Cluster in EC2 instances

B) Develop and Deploy sample application

Sample shopping cart application is created and deployed in cloud environment to enable testing. Angular SPA application framework is used for sample application. This application will be deployed in AWS EC2 cluster environment.

C) Broker Creation

Broker is external piece to the application. Broker takes care of security issues, cloud service provider selection, validates user request etc. Since broker is entry point for applications, this is made even more important component by deploying machine agent in it.

- Create broker application
- Deploy Broker in EC2
- Deploy Machine Agent rules in Broker
- It acts like a proxy kind of thing (multiple rules)

D) Machine Agent

In Traditional approaches, Machine agent will be deployed in every server for validating the incoming request. In this paper, machine agent in broker is deployed as broker is entry point. Hence this reduces multiple machine agent deployments and also makes application more secure.

- Machine Agent will be deployed with defined rules
  - ✓ SQL Injection
  - ✓ DDoS (Denial Of Services)
  - ✓ Flooding Attack
  - ✓ Blacklisted IP

E) Feedback Providers

Feedback providers add integrated feedback mechanism in proposed system. This will receive continuous blacklisted IP and White listed IP's. This will be integrated in machine agent deployed in Broker. Hence machine agent can use this system to add more security to the system

- ✓ Provide frequent blacklisted IP
- ✓ Provide white listed IP
- ✓ Abnormal Text in Request
- ✓ Allows only authorized users.

F) Trust Validation

Proposed trust validation is different from traditional approach. Here in applied both real time data and cloud user rating mechanism to calculate the trust value of service provider. Project methodology is discussed in detail as below.

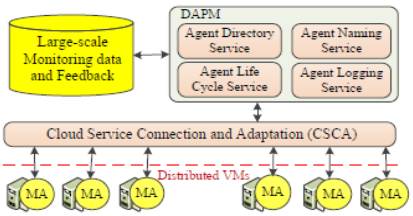
- ✓ Data-driven Trust Computation
- ✓ Enhanced and Hierarchical Feedback Mechanism
- ✓ Identifies blacklisted ip
- ✓ Identifies unauthorized users.
- ✓ Validates proper request parameters.
- ✓ Does the about validation using decision tree algorithm.

Data Driven Trust Validation

To guarantee quality of service from with respect to resource trust worthiness, parameters such as CPU, memory, IO, response time etc. are monitored as detailed below.

Monitoring indicators of trusted cloud services

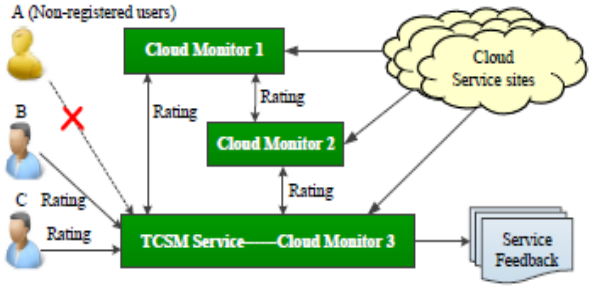
Trust attributes	Monitoring data
resource service attributes (dynamic values)	I_1: current network bandwidth I_2: current CPU utilization rate I_3: memory utilization rate I_4: hard disk utilization rate I_5: average response time I_6: average task success ratio



4. RESULTS AND DISCUSSIONS

a) Enhanced and Hierarchical Feedback Mechanism

This Feedback mechanism is based on user rating. User rating will be consolidated for every transaction after end of service request. This will be used for future service request. Hence poor service will be ignored.



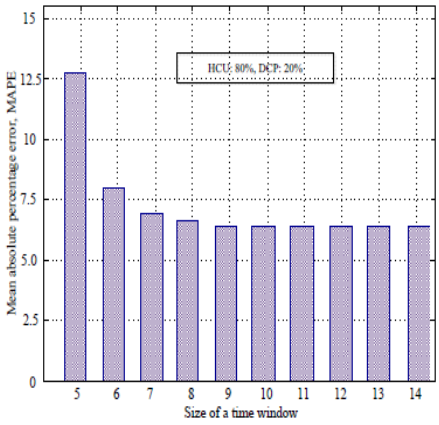
b) Accuracy Evaluation

Formula for evaluation error to reflect the system's accuracy is introduced. For a given cloud resource (service) Ni, the Mean Absolute Percentage Error (MAPE) is defined as:

$$\mathcal{MAPE} = \left(\sum_{t=1}^{n} \left|\frac{\mathcal{F}_{t+1} - \mathcal{F}_t}{\mathcal{F}_{t+1}}\right|\right) \times 100 \Big/ n$$

$$= \left(\sum_{t=1}^{n} \left|\frac{\xi_t}{\mathcal{F}_{t+1}}\right|\right) \times 100 \Big/ n$$

where ξt is the evaluation error in the t-th test, ξt = (Ft+1−Ft), Ft+1 is the actual value calculated by the trust system in the (t+1)-th test, and Ft is the calculated value in the t-th test. n refers to the total number of evaluation. The value of MAPE is an indicator of accuracy in trust evaluation. MAPE is verified to determine whether the accuracy is within the acceptable control limits.



Sliding time window mechanism is used to reflect the dynamic nature of trust, which is one of the main features of this work. Experimental results under different sizes of time window Δt are observed. The experimental environment is a more stable community environment, in which 80% of CUs in the cloud market are HCUs, and 80% of CPs always provides stable service. In this experiment, Δt is defined with possible values ranging from 5 to 14. From the experimental results in Fig, when the value of the parameter Δt is less than 10, the values of MAPE are the lowest compared with other values of Δt. When the value of parameter Δt is higher than 10, the values of MAPE change in a flat trend. From the experimental results in Figure, higher values of Δt result in better performance in terms of accuracy. However, in a cloud market with large-scale transactions, a higher Δt may result in larger time and space overhead. According to the results in Figure, it is suggested to set Δt = 10 as the compromising value for this parameter.

5. CONCLUSION

In the proposed system, broker is enabled as secured gateway by deploying machine agent in it. This proves more efficient methodology to avoid cost and resource usage of machine agent deployed in many server instances. Additionally this keeps application as security layer is moved one step ahead. Along with this application resources are also freed up as CPU and memory consumption of application hosts will be used only for application execution. This methodology effectively segregates application and security layer.

REFERENCE

[1] C. Ngo, Y. Demchenko, and C. de Laat, "Toward a dynamic trust establishment approach for multi-provider intercloud environment," in Proc. 4th Int. Conf. Cloud Comput. Technol. Sci. (CloudCom), Dec. 2012, pp. 532–538.

[2] R. Parameswari, G. C. Priya, and N. Prabakaran, "A trust, privacy and security infrastructure for the inter-cloud," Int. J. Comput. Technol. Appl., vol. 3, no. 2, pp. 691–695, 2012.

[3] X. Li, H. Ma, X. Gui, and W. Yao, "Data-driven and feedback-enhanced trust computing pattern for large-scale multi-cloud collaborative services," IEEE Trans. Serv. Comput., to be published, doi: 10.1109/TSC.2015.2475743.

[4] I. Butun, M. Erol-Kantarci, B. Kantarci, and H. Song, "Cloud-centric multi-level authentication as a service for secure public safety device networks," IEEE Commun. Mag., vol. 54, no. 4, pp. 47–53, Apr. 2016.

[5] H. F. Mohammadi, R. Prodan, and T. Fahringer, "A truthful dynamic workflow scheduling mechanism for commercial multicloud environments," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6,pp. 1203–1212, Jun. 2013.

[6] F. Paraiso, N. Haderer, P. Merle, R. Rouvoy, and L. Seinturier, "A federated multi-cloud PaaS infrastructure," in Proc. 5th IEEE Int. Conf. Cloud Comput. (CLOUD), Jun. 2012, pp. 392–399.

[7] H. Shen and G. Liu, "An efficient and trustworthy resource sharing platform for collaborative cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 4, pp. 862–875, Apr. 2014.

[8] X. Li, H. Ma, F. Zhou, and W. Yao, "T-broker: A trust-aware service brokering scheme for multiple cloud collaborative services," IEEE Trans. Inf. Forensics Security, vol. 10, no. 7, pp. 1402–1415, Jul. 2015.

[9] X. Li, H. Ma, F. Zhou, and W. Yao, "T-broker: A trust-aware service brokering scheme for multiple cloud collaborative services," IEEE Trans. Inf. Forensics Security, vol. 10, no. 7, pp. 1402–1415, Jul. 2015.

[10] M.Ulema, M. Waldman, and B. Kozbe, "A Framework for Personal Mobile Agents in Wireless Pervasive Computing Environment," Proc. Int'l. Symp.Wireless Pervasive Computing 2006, Phuket, Thailand, 16–18 Jan. 2006.

[11] Butun, B. Kantarci, and M. Erol-Kantarci, "Anomaly Detection and Privacy Preservation in Cloud-Centric Internet of Things," IEEE ICC 2015 — 1st Wksp. Security and Privacy for Internet of Things and Cyber-Physical Systems, London, U.K., 2015.

[12] R. Khan, R. Hasan, and J. Xu, "SEPIA: Secure-PIN-Authentication-as-a-Service for ATM Using Mobile and Wearable Devices," 2015 3rd IEEE Int'l. Conf. Mobile Cloud Computing, Services, and Engineering, Mar. 2015,pp. 41–50.

[13] B. Kantarci, M. Erol-Kantarci, and S. Schuckers, "Towards Secure Cloud-Centric Internet of Biometric Things," IEEE Intl. Conf. Cloud Networking, Oct. 2015, pp. 182–84.

[14] X. H. Le et al., "An Energy-Efficient Access Control Scheme for Wireless Sensor Networks Based on Elliptic Curve Cryptography," J. Communication and Networks, vol. 5, no. 3, 2009.

[15] Z. Benenson, N. Gedicke, and O. Raivio, "Realizing Robust User Authentication in Sensor Networks," Proc. Wksp. Real-World Wireless Sensor Networks, 2005

[16] H. R. Tseng, R. H. Jan, and W. Yang, "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks," Proc. IEEE GLOBECOM, 2007.

[17] R. Buyya, R. Ranjan, R. N. Calheiros. Inter Cloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services. 10th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP), Busan, Korea, 2010.

[18] S.K. Nair, S. Porwal, T. Dimitrakos, A.J. Ferrer, J. Tordsson, T. Sharif, C. Sheridan, M. Rajarajan, A.U. Khan, Towards Secure Cloud Bursting, Brokerage and Aggregation. In: 8th IEEE European Conference on Web Services (ECOWS 2010), pp. 189-196, 2010.

[19] N. Andelman, Y. Azar, and M. Sorani. Truthful Approximation Mechanisms for Scheduling Selfish Related Machines. In Proceedings of the 22nd Symposium on Theoretical Aspects of Computer Science, 2005.

[20] N. Jain, I. Menache, J. Naor, and J. Yaniv. A truthful mechanism for value-based scheduling in cloud computing. In SAGT, pp. 178-189, 2011.