SecureTrustManagementinMulti-CloudEnvironment

P.REVATHI [1], MUTHTAMIL V [2]
[1]Assistant Professor, Department of ECE,
[2]Assistant Professor, Department of CSE,
[1,2]Dhanalakshmi Sirinvasan College of Engineering and Technology, Chennai

ABSTRACT

Managing trust in cloud environment is the biggestobstacles in its adoption and increase in popularity among theclients.Sincethecloudserviceusershavetoshareall theirconfidential data with the cloud service providers, hence, it isobvious that they will choose service providers that are reliable.This article describes a solution for the problem of evaluating anunbiased subjective trust.Wehavedescribedamethod thatdivides the users chosen for feedback into two groups. Thesegroups are interviewed by the trust service providers. These arethe people who provide the trustworthiness and reliability of thecloud service providers. These trust ratings are provided basedon two things. First the feedback from different cloud serviceusers. These users are divided into two groups. Firstly, the userswho have used the service in their past. And second, the userswho are currently using the services. Next measure is how wellthatcloudserviceprovideradherestotheservicelevelagreement.

INTRODUCTION

Cloudcomputingbecomesasubstitutecomputingparadigm to offer varied and on-demand resources, code, andplatform as a service. It can be a model for an easy, sanctionnativepresenteverywhere,on-demandnetworkaccesstoacommon pool of computing resources that are able to configure(e.g.networks,servers,storage,applications,andservices)which will be provisioned readily and dismissed with minimalmanagementattempts.Cloudcomputingoffersservicedynamism,flexibilityandlargechoiceo fdecisionstoenterprises.Intoday'scompetitivesurroundings,enterprisescannotignoretheseservices. Versatilecloudcomputingservices need one party (i.e. Cloud shopper) believe the actionsof different party (i.e. Cloud Service supplier), therefore, trusthasbecomeanimportantelementofsuchservicesfromsecurity purpose of customers. It is an innovative means ofdelivering scheming resources for executing web applicationsandinternetsites.

Cloudcomputingoffersserviceslikewebmail,blog,storage, hosting services on internet, infrastructure, platformand software services for fulfilling the needs of patron. It ismainly a mixture of current technology which has proven to beskilfulinmakingdistributedsystems,digitalcomputer,virtualizationandnetworkstorageofdistribute dknowledge.

OBJECTIVES

Mostly cloud computing provide outsourcing services on-demandlikesoftwarepackage,platforms,applications,infrastructure, business and data etc.It offers the support ofservicerequestofresourcestopurchasers.Itsassociatedapproach where there is provision of pooling of computingresources to provide dynamic, shared and versatile resourcesthroughInternet.Cloudcomputingusesthebasicsofdistributedcomputing,virtualization,grid computing,serviceorientationetc.Theservicesprovidedbythecloudcanbebroadly classified into three categories: Software as a Service(SaaS), Platform as a Service (PaaS), and Infrastructure as aService(IaaS).

PROBLEM STATEMENT

They have devised a basicpattern of solution that can facilitate to service users. Theirsolution completely altered the administration domain. Due tothis transfer, cloud service user had control over the data. Theproposed framework provides not only trust rating identifyingandeliminatingobjectionsbyevaluatingthecompatibleproblems of creating confidence in the system of cloud. Theyhave given the different methods for transferring the controlfrom service providers to the providers but also transfers theadminpowertothecontrolofcloudusers.

An algorithm for confidence level scheduling in cloud hasbeen devised by the authors in. It is calledas dynamictrust level scheduling (DLS) for the cloud computing. Bayesiancognitivemodelisbeingusedtoprovidetherelationshipmodel of sociology. First, an innovative Bayesian method isbeing proposed depending on the cognitive trust model. Then,current DLS algorithms are mixed to propose an algorithm fortrustdynamiclevelscheduling.Experimentalanalysis(theoretic as well as simulation) shows that Cloud-dynamictrustlevelschedulingalgorithmcansatisfytheworkloadsrequirementofcloudinconfidenceandtheachievementofjobs is assured in a protected way. At the same time, it offerslessdependability,integrity,safetyandconfidentiality.

Asystemthatismanagingtrustinthe environmentofcloudwhichfocussesoverthedatamixingwiththeappsintheenvironmentofmobile cloud. They have attempted to develop a system thatapproaches to exploit the fundamentals of the trust servicedframework and it is incorporated in the environment of mobileapp. For this they have to shift their focus to the mobile device.Hence, they had to monitor the mobile devices and verify theusers'interactioninthemobileenvironment.

OVERVIEW

From the diagram we can see how the various actors are placed in a system model that performs the task of trust evaluation in a multi-cloud framework for the cloud service providers. This framework or model not only evaluates the trust values of the service providers but also is capable of providing the on- demand trust values. The main actors involved in a trust management framework involving TSPs are: CSPs, CSUs and TSPs themselves. Below is the description of main actors and their activities.

CSPs or cloud service providers are the companies that provide the cloud services to the cloud service users. The CSPs generally offer a set of facilities and these facilities are written in SLA or service levelagreement, as displayed in Fig.

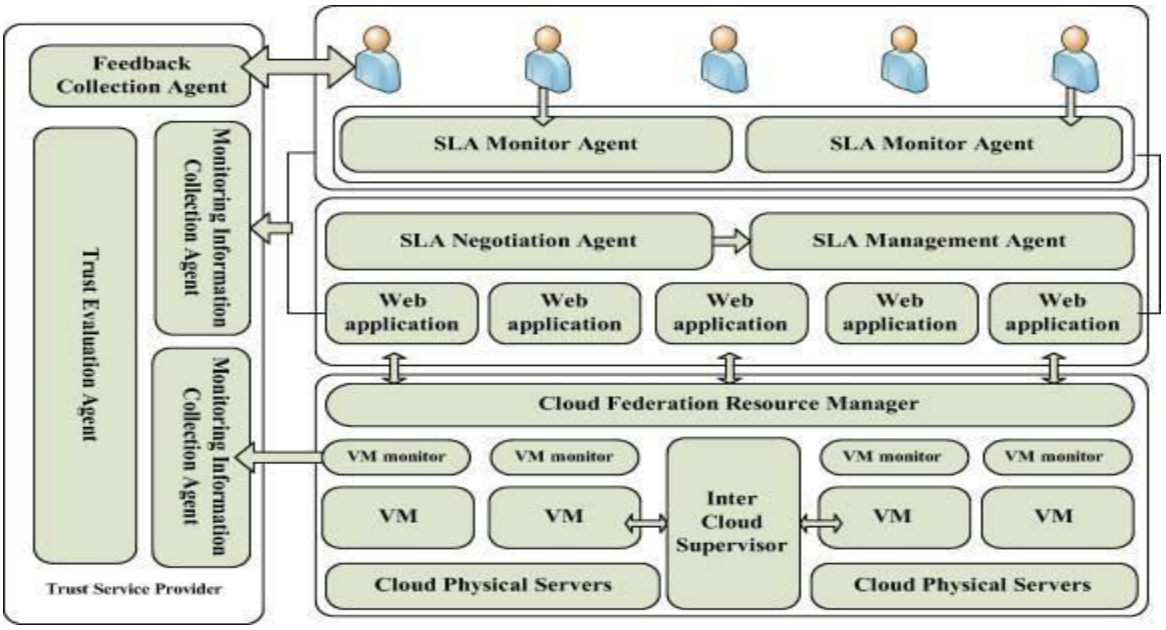
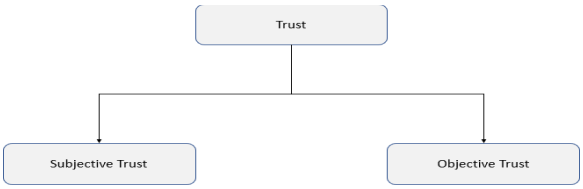


Fig : System Architecture

.PROPOSEDSYSTEMMODEL

Theproposedsystemmodelexploitsthevulnerabilitythatfeedbackfromthecloudserviceuserscanbebiase dinamanner or another. So, to evaluate the trust which is subjectivein nature, we cannot fully rely on single cloud service user.Also, in the use of a particular cloud service provider services,thedataofthatcloudserviceuserliesincontrolofthatparticularcloudserviceprovider.

Themainframeworkforevaluationofthetrustrevolves around the evaluation of the subjective trust and theobjectivetrust,asshown inFig.



ProposedEvaluationModel

Let us consider we have two groups labelled as group A andgroup B. As shown in Fig, members of group A are thecurrentusersandmembersofgroupBarepastusers.
Let us consider there are ‘n’ members in group A and ‘m’membersingroupB.
So,

Nowif|Ra-Rb|<1wehaveunbiasedratings.Elseweincreasenandm.
IfcomputationtimeforeachmemberofAistaandforeachmemberofBistbthentotalcomputationtim
eis,

Tp=ta×n+tb×m □□□

Sinceexistingmodeldoesnothaveasetofexistinguserssowecansaythattheapproximatecomputati
ontimeforthemis-

Te=ta×n

Sowecanseethat,

Tp>Te

A={a1,a2,a3,… ,an}
B={b1,b2,b3, ,bm}

CONCLUSION

Trustevaluationmodelismuchimportantincloudcomputing.An evaluation model of trust depending on the subjective andobjective trust has been described in the paper. The devisedmodelhasseveraladvantages.Itiseasytoexecute.Theobjectivetrustpurelydependson themonitoringofthequalityof services provided by the cloud service providers and alsoverifying if they are providing all the services listed in theservicelevelagreement.

REFERENCES

[1] Z. Cao, H. Guo, J. Zhang, D. Niyato, and U. Fastenrath, "Improving the efficiency of stochastic vehicle routing: A partial Lagrange multiplier method," Vehicular Technology, IEEE Transactions on, vol. PP, no. 99, pp. 1–1,2015.

[2] Ming Yu, Kin K. Leung "A Trustworthiness-Based QoS Routing Protocol for Wireless Ad Hoc Networks," IEEE Transactions on wireless communications, vol. 8, no. 4, April2009.

[3] M. Lin, L. Xu, L. T. Yang, X. Qin, N. Zheng, Z. Wu, and M. Qiu, "Static security optimization for real-time systems," IEEE Transactions on Industrial Informatics, vol. 5, no. 1, pp. 22–37, Feb2009.

[4] Yih-Chun Hu, Adrian Perrig "A Survey of Secure Wireless Ad Hoc Routing Published," by IEEE security & privacyIEEE-2004.

[5] RakpongKaewpuang, DusitNiyato, Ping Wang and Zhu Han "Optimal Decentralized Security Software Deployment in Multihop Wireless Networks" IEEE Globecom 2014 - Communication and Information System SecuritySymposium.

[6] NageshNandiraju, DeeptiNandiraju, Lakshmi Santhanam "Wireless Mesh Networks: Current Challenges And Future Directions Of web-in-the- sky" IEEE Wireless Communications August2007.

[7] Patrick Tague, David Slater and Jason Rogers "Evaluating the Vulnerability of Network Traffic Using Joint Security and Routing Analysis" IEEE Transactions on dependable and secure computing June 2009.

[8] Xiangqian Chen, Kia Makki, Kang Yen, and NikiPissinou"Sensor Network Security: A Survey" IEEE Communications Surveys & Tutorials Vol. 11, no. 2, Second Quarter2009

[9] Stefano Paris, Cristina Nita-Rotaru, Antonio Capone "Cross-Layer Metrics for Reliable Routing in Wireless Mesh Networks" IEEE/AcmtransActions on Networking, Vol.21, no.3, June