Research on Trust Computing for Cloud Service Providers

V. Punithavalli, P. Sheela Gowr, M. Latha

Abstract--- ***Cloud computing has evolved over a decade and thrived to the state that Information Technology cannot survive without cloud. It has evolved in such a way that it is embedded in every one's life. Though cloud has become integral part of every new software, still there are gaps in security features and customers keenly look into multiple aspects of cloud service provider features before choosing their appropriate CSP. More than cost and features Cloud Service Provider should gain trust of the clients to do more business. There are lot of factors involved to gain confidence of client such as transparency, cost, security etc. Also how flexible the provider can help in deploying for various light weight devices such as Internet of Things (IoT) also matters where in IoT is emerging industry. Concurrently Cloud Service capability to work in collaborative fashion and other machine learning features will also take into account by clients to choose their respective best fit Cloud Service Provider.***

Keywords--- ***Trust Computing, Cloud, Broker, Secured Cloud.***

1. INTRODUCTION

Big Data, Data Mining, Machine Learning and Internet of Things (IoT) are evolving and been used in Many enterprise applications and day to day applications. These technologies create lot of data. With Internet of Things various sensor data is getting generated at very high space. These data needs to be stored and process at high pace. Existing database technologies and computing capacity are not capable to support these. Hence Big Data and data mining technologies are mostly used in these scenarios. Additionally machine learning is required in various use cases to identity meaningful information from large amount of data. This requires more computing capacity. With current systems not capable enough to support computing capacity, clients look for Cloud Service Providers for computing these data.

With customers choosing Cloud technology for high processing capability, there were lot of features provided by CSP's to promote customer migration from local hosting to cloud hosting. Cloud Service provides cost benefit in terms of Infrastructure maintenance, Infra cost and other benefits. Additionally they provide more security features and easy application scalability features. Every cloud service providers increase their security feature and easy deployment features, more data transparency to gain customer trust.

Below are key parameters in trust computing for CSP.

Quality of Service (QoS): Quality of Service is one of the key components to measure trust computing. Most reliable and more robust platform will gain more confidence of the customer. This service will be more preferred and chosen by customers.

Continuous Feedback: Trust will also be obtained by peer customer reviews. Customers before choosing services will go through prior customer. Continuous feedback and cloud automatically choosing best service for customer will be more preferred. These will help in gaining more confidence.

Transparency: Customers of Cloud are exposing their data outside their network. In many cases customer might not know how secure their data is. This is very critical factor for all cloud applications. Cloud Service Provider should make sure that proper auditing is done so that customer feels safety on data aspect.

Light Weight: With Internet of Things evolving, these devices need lot of security features enabled at cloud layer. Since IoT devices lack more computing capacity, adding security for these are IoT are complex at device end. At the same time they should respond fast enough. Hence customer chooses best service provider who provides where light weight security is enabled.

2. RELATED WORK

Khan and Malluhi have studied cloud service provider features on security aspect. They took into picture what are the needs of cloud users and validated them against features provided by Cloud Service Provider in terms of privacy to data. On their study, they have identified important items considered by Cloud user. They have stated that ownership, control, security and prevention as very important items considered by Cloud user. These factors will determine the trust factor of user on Cloud Service Provider. Service provider trying to restrict user control on data and restricting transparency will impact user's trust on Cloud Service Provider. To increase user's trust, Service Providers should enable below

1. Remote access for user's resources
2. Transparency by enabling traceability
3. Certification on Security aspects from independent certification authority

Signal came with new idea of proxy based approach where multiple clouds where used in collaborative approach. This framework will enable below without prior collaboration agreement.

1. On the fly resource sharing among multiple CSPs.
2. Trust policy
3. Privacy issues

Revised Version Manuscript Received on April 12, 2019.

V. Punithavalli, Student, Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamilnadu, India. (e-mail: vpunithavalli27@gmail.com)

P. Sheela Gowr, Assistant Professor, Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamilnadu, India. (e-mail: sheela.se@velsuniv.ac.in)

M. Latha, Assistant Professor, Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamilnadu, India. (e-mail: latha.se@velsuniv.ac.in)

Author also strongly recommends that while involving multiple cloud providers, trust among cloud service should be established and this must undergo rigorous analysis. These rigorous approaches will un-earth potential threats and concerns in collaboration approach. These should be supported by innovation in these areas. Re-usable mechanism should be identified to provide more effective privacy and security for application data. These mechanisms will gain enabling customers to adopt new technologies easily.

Liu and Shen came up with new approach named ‘Harmony’. Harmony is an approach to build more trusted sharing platform in a collaborative environment for cloud. This is enabled by integrating reputation and resource management in harmonious fashion. This approach will help to derive joint management in environment where multiple clouds are involved. Harmony has different approach from prior resource management and reputation management. In Harmony approach a node is dedicated to locate resource and also identify reputation of that resource. This enables the users to choose the required resource not just based on the availability of the resource. With this approach, user has the flexibility to choose the resource based on availability and reputation too. In this approach, trust factor will be calculated based on weighted average method.

Attack Pattern Analysis. This study will help in understanding how system secures itself from various malicious attacks. Cloud user would prefer to store data in environment which is considered to be safer. Hence it is very important factor for all cloud service provider to secure it from various malicious attacks. In collaborative environment where multi cloud interact with each other attack can come from unknown network or selfish sites hosted within environment. System should be capable to identify Garnished attacks. Garnished attacks are mostly from selfish sited that might look good but attack within network without being un-noticed. Cloud Service Providers should have appropriate mechanism to avoid these kinds of internal attacks to maintain their trust factors.

3. MATERIALS AND METHODS & RESULTS

DFET has come as an alternative approach to most recent studies that were focussed on single sided trust evaluation factors. DFET pattern is hybrid approach to measure trust. Trust worthiness of cloud service provider is measured from below key components

1. Quality of Service(QoS)
2. User feedback / monitor feedback

These factors can solve issues from one sided trust computing model. DFET approach is comparatively consistent with prior approached in deriving trust relationship with necessary attributes of trust. This falls more in line with end user expectations and needs. DFET approach also uses TTP as its backbone. Various other models uses only trust factor derived at user end which is an additional load to user. In TTP, it used cloud monitor where more services are registered. TTP helps in providing additional feedback. This helps to reduce user load and also increased trust calculation accuracy.

Data-driven Trust Degree (DTD) is a new approach that dynamically calculates satisfactory and un-satisfactory services. DTD follows sliding window mechanism. Pre-defined time window of specific duration will be set. Satisfactory services and un-satisfactory services will be measured in the time frame of specified time window. SSD will be measured in the specified time window frame. Once time frame elapses, sliding window mechanism will shift time frame towards right side. It drops the service behaviour measured in the prior time frame. This mechanism forgets the prior measurement and adds new measured from current time frame window. Time window frame can be increased or decreased based on scenario to scenario.

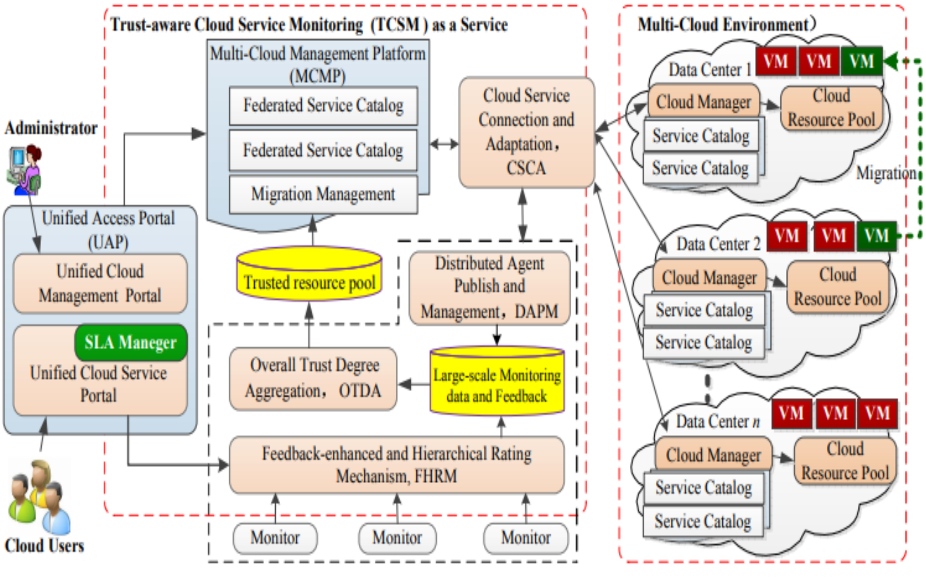
Trust-aware Cloud Service Monitoring (TCSM) as a Service
Multi-Cloud Management Platform (MCMP)
Federated Service Catalog
Federated Service Catalog
Migration Management
Cloud Service Connection and Adaptation, CSCA
Administrator
Unified Access Portal (UAP)
Unified Cloud Management Portal
SLA Maneger
Unified Cloud Service Portal
Trusted resource pool
Distributed Agent Publish and Management, DAPM
Overall Trust Degree Aggregation, OTDA
Large-scale Monitoring data and Feedback
Feedback-enhanced and Hierarchical Rating Mechanism, FHRM
Monitor
Monitor
Monitor
Cloud Users
Multi-Cloud Environment)
Data Center 1
VM
VM
VM
Cloud Manager
Cloud Resource Pool
Service Catalog
Service Catalog
Migration
Data Center 2
VM
VM
VM
Cloud Manager
Cloud Resource Pool
Service Catalog
Service Catalog
Data Center n
VM
VM
VM
Cloud Manager
Cloud Resource Pool
Service Catalog
Service Catalog

Fig. 1: Trust aware cloud service Monitoring

Inter-Cloud Trust Model is one of trust computing model for Cloud Service providers. With respect to PKI model, root will enact as Authority centre to establish trust between different inter cloud parties.

The Authority Centre will issue enact as Certificate Authority (CA). Certificated received by inter cloud parties from Authority Centre needs to be handshaked between these parties to ensure trust. Defined by architecture, Authority centre will be intermediated authority in establishing trust for lifetime of transaction. Inter cloud parties will have their own responsibility of establishing trust dynamically on top of PKI trust model. Most models are domain based models. Hence cloud service provider environments will be distributed into several nodes and domains. Similar domains share familiarity and enjoy higher trust factor between them.

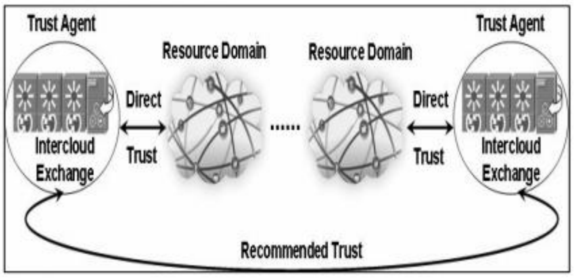

Fig. 2: Inter Cloud Trust Model

Inter-Cloud Trust Model

Celesti et at came up with key factor to successfully manage identities. In cloud environment where multiple parties form an Inter Cloud environment, client supports standard frameworks such as WebService, Security Assertion Markup Language (SAML) and ID-FF (Identity Federation Framework). Multiple standards provide well defined frameworks to establish authentication, authorization, Role management, Data Integration, virtualization etc. To establish communication between inter cloud parties; they should start with requesting a trust token. When receiving trust token request, service poviders needs to share secret keys to requested consumer. In the communication chain, if the requestor is involved with another cloud exchange, XMPP server will send message to recipient XMPP server. In communication between inter cloud parties; server will accept connection only when certificate handshake is successful.

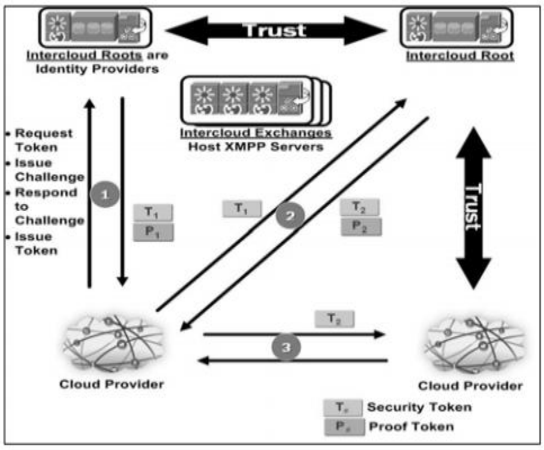

Fig. 3: Inter Cloud Root and Inter Cloud Exchange Collaboration

4. CONCLUSION

As cloud computing is dominated in all domains, it required to follow standard procedures to establish security between cloud environments. Here comes third party certification to make sure that security requirements are met. Identity management is an early challenge that must be resolved since identification and authentication must be performed not only for customers and users, but also for resources as well within heterogeneous cloud environments. In this paper, we have studied multiple trust computing models evolved over years in the field of cloud computing. We observed many technologies considering feedback of users and intermediate agents more effective than others.

REFERENCES

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. 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. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. B. Kantarci, M. Erol-Kantarci, and S. Schuckers, "Towards SecureCloud-Centric Internet of Biometric Things," IEEE Intl. Conf. Cloud Networking, Oct. 2015, pp. 182–84.
12. 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.

13. Z. Benenson, N. Gedicke, and O. Raivio, “Realizing Robust User Authentication in Sensor Networks,” Proc. Wksp. Real-World Wireless Sensor Networks, 2005
14. H. R. Tseng, R. H. Jan, and W. Yang, “An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks,” Proc. IEEE GLOBECOM, 2007.
15. 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.
16. 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.
17. 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.
18. 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.