Indian Journal of Science and Technology, Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/108685, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Survey on Trust Models in Cloud Computing

K. Gokulnath[1]* and Rhymend Uthariaraj[2]

[1]Parul University, Vadodara – 391760, Gujarat, India; kgnathit@gmail.com
[2]Anna University, Chennai – 600025, Tamil Nadu, India

Abstract

Objectives: Objective of this work is to explore the available solutions for cloud trust and thereby to facilitate a rigid solution to address the issue in future. **Methods/Statistical Analysis**: Cloud Computing caters dynamic resources and on-demand services without the overhead of license, purchase and other traditional IT administration activities. Cloud is not only a buzz word in the industry but, also a most happening technological trend. While the services provided by the Cloud Computing is surplus, concern over the promising aspects are of no doubt. The barricades to cloud implementation in the reality are abundance. **Findings:** Amongst the barricade to cloud implementation, security and trust are considered to be the foremost issues. Trust is always a worry for the new technologies and also for distributed computing paradigm. Prospective users to Cloud Computing shall be tapped in only if the issue is precisely addressed. Minimizing the investment cost is one of the key features promised by the cloud vendors. Any security compromise towards minimizing the cost is highly intolerable. A trust solution for the Cloud Computing should balance the users worry towards trust as well as the service provision aspect. There are several promising solution to cloud trust problem exists**. Application/Improvements:** This work weighs some of the solutions to cloud trust and thereby highlights the potential gap between the actual requirement and the real solutions.

Keywords: Cloud Survey, Cloud Survey, Cloud Trust, Cloud Trust Challenges, Cloud Trust Issues; Trust Survey

1. Introduction

With the advent demand for computing grows exponentially, need for computational resources becomes basic necessity. Cloud Computing caters to the diverse computational needs for consumers. Though, the model of Cloud Computing offers on-demand dynamic computational capability, usage of Cloud Computing still needs improvement. Major concern over the usage of cloud is trust and security. Cloud Computing offers sophisticated security methods to keep away the intruders. Still the concern of trust over the specific issues related to cloud like third party domain, multi tenancy, availability, reliability, etc. needs to be answered to greater extent. Even though more users are getting adapted to cloud environment, huge gap exist between actual utilization to capabilities.

While the task of attracting the potential consumers overcoming the trust concern who are not into the cloud is a mighty task, other side of it does exist. Consumers who are already into the cloud face the challenge of internal and external threats within and outside the organization. A survey[1] reports at least 14% of the internal threats in the year of 2014 for cloud users are internal data threats. The same threat is extended to a vast 61% minimum for the data owned by cloud. With these statistics in hand 41% of the corporate are moving to cloud with caution. Reasons cited for non usage of Cloud Computing is the barricades and it counts to 73%. The percentage figures in the survey[1] counts to the global community, regardless of the geographical domain.

In another interesting survey[2] less than 10% of the total apps are reported to be in cloud. Sensitive data that are uploaded is reported to be less than 10% again. Another statistics states that as little as less than 5% respondent uploads their sensitive data to outside organizations or unauthorized individuals.

*Author for correspondence

It is clear from the statistics[1,2] that demand for resources from Cloud Computing is restricted in spite of actual capabilities. All the services offered from cloud, IaaS; SaaS; PaaS, suffers under utilization of the actual capable resources. Thus it is mandatory to come up with some sort of solutions for the enhancement of better utilization of the cloud resources. Until the barricades to trust are attenuated, realization of benefits will be restricted to greater extent. Distributed computing paradigm suffers this initial lack of trust traditionally. Proven methods to establish trust in traditional environment may not be suitable for cloud because of cloud's dynamic nature.

This work collects and weighs the available methods in the literature for establishing trust in cloud environment. Also this survey identifies the merits and demerits through careful analysis of the available methods. Due experiments are conducted for testing the behavior of the available methods.

Rest of the work is organized with the continuation from this section as Section 2 describes the generic barricades to cloud trust and Section 3 briefly explains the available methods in the trust on cloud environment. Section 4 summarizes the methods and identifies some scope of extending the methods available to enhance the trust further. References made for this work is listed at last.

2. Barricades to Cloud Trust

As introduced in previous section there are various factors cited by cloud users[1,2], that restrict them from potential benefits. Trust is defined as the continuous expected behavior of an entity. Here, in Cloud Computing too trust is a dynamic entity. Trust in cloud is the expected continuous behavior of the service provider (Users perception). Since, cloud is a dynamic computing paradigm behavior of cloud is also dynamic. This dynamic nature of Cloud Computing is applicable for trust also. But, an entity can be trusted if and only if it poses steady state characteristic. All these attributes makes trust as a challenging factor in cloud environment. Below discussed are some factors that make it more difficult to model cloud trust.

2.1 Control

First and foremost barricade to Cloud Computing is the concern over control or ownership. Since the computational resources, data, platform and several other key attributes for computing are owned by the third party resources, the trustworthiness of the system is obviously in the limelight. A report[2] says cloud users are not willing to blindly believe the cloud resources. Prospective cloud users shall be tapped in only if the concern over third party ownership is addressed properly through the Service Level Agreement (SLA). Control over the attributes within other domain and cross administration policies are not a lighter process to be levied to the users.

2.2 Privacy

Cloud Computing is better known for its multi-tenancy. This property of the cloud has given room for enormous concern over the privacy of individual users and corporate. The probability of two competing users or corporate residing in the same Datacenter is possible. In this situation the key question is how the service provider (Datacenter) do segregates the individuals. SLA should be in place to clarify the segregation strategy. The technology adapted to address segregation and its associated methodologies must be specified and briefed in detail in SLA.

2.3 Reliability

SLAs must carry the delivery measures of the erroneous situations are to be handled than compensating or penalizing the cause. Most of the services provided through clouds are real time hence, a way to ensure reliable service delivery is mandatory. To be precise preventive mechanisms like vm migration policy (in IaaS), data backup stores (in PaaS), checkpoint computations (in SaaS), etc. are to be mentioned mandatory in the SLA, before the commencement of services. Unless precautionary measures are not specified in the SLA, attracting mass customers are highly difficult.

2.4 Security

Securing the clients information is always a pivot task in any form of computing. In Cloud Computing since the usage of virtual machines gets into picture, tackling the security by traditional approach may not be appropriate. Thanks to the sophisticated encryption like homomorphic encryption techniques. Associated issues like integrity, authenticity, access control mechanisms are to be given due consideration. Otherwise working in external systems may not yield the desired results in fact it may turn to be disastrous.

In general evaluating the specific cloud service provider needs multiple parameters. For instance, the service provider who provides excellent infrastructure services (IaaS) may not be ascertained for other (SaaS and PaaS) types of services. The service provider providing similar kind of service needs designated amount of transactions, number of entities served, time of existence, etc. and other user defined attributes for absolute verification. Available methods do poses these characteristic and still attentions required to enable cloud platform as most trustworthy as traditional. Works are in progress to address the stated issues and answer the queries raised by the cloud user's trust. Objective of the Cloud trust is to increase potential cloud users against the current usage statistics stated[2]. Service Level Agreement (SLA) is the link that portrays the capability of the service provider. Hence, these methods are adopted to deploy trust before the instigation of the services.

3. Trust Models in Cloud

Dynamism in Cloud Computing pose serious concern to trustworthiness. Resource behaviors vary with respect to time and applications, not only the resources, even the users are not regular. These aspects are common among various distributed systems. Cloud is even more dynamic with the use of virtualized computations involved. Thus, these characteristic make trust as a limelight problem from both user and resource provider's perception. Classical solutions do exist to establish trust among the distributed system but mapping the solutions to cloud is restricted by several parameters. This section highlights some of the solutions for the trust evaluation in cloud environment.

3.1 Feedback Model

Most common method among the distributed system is to collect the feedback of a target system and rate it accordingly and termed as feedback based trust establishment. Several of the trust establishment methods like in[3–8] establish trust between cloud user and service provider. There are two different methods in feedback approach.

- Direct Method.
- Indirect Method.

3.1.1 Direct Method

In direct method, cloud users have past transaction history with the service providers, based on the service credentials, service providers are sorted according to the degree of service satisfaction. Sorting of service providers are carried mostly in descending order. Scaling for achieving the ordinals of service providers are carried by continuous or discrete scale of values. Most preferred type of ordinals is continuous scale. Say, for example a continuous scale of 1 to 5 or 0 to 1 is preferred. A minimum threshold of service satisfaction is fixed initially. Several experiments are carried to fix the minimum threshold level. Since the cloud is dynamic distributed system, the threshold may vary from time to time and from system to system. In general, 85% and above valued systems from feedback are classified as tier-1 systems. Tier-1 systems are designated as most trusted systems. Value of 4.25 and above in a 1-5 continuous scale and 0.85 and above in 0-1 continuous scale is the sample range. Most of the systems may not fall in this category because of various reasons. Hence, second level of systems may carry the value between 70% to 85%. Eventually, 70-85 % levels of ordinal systems are designated as tier-2. Tier-2 systems are considered as simply trusted systems. Values are 3.5 and above in a continuous scale of 1-5 and 0.7 and above in 0-1 continuous scale. Also, there are tier-3 systems lesser than 70%, named as untrusted systems and tier-4 systems totally untrusted systems. Gross threshold limits may vary as insisted earlier; core idea is to segregate the systems according to the level of service satisfaction. Here the core idea of calculating the trust value of the system is depicted; due assumption is system posses past history of transaction with the target system. Let n be the total number of systems offering the cloud service, i denotes the current iteration, k denotes the system of interest, t be the trust value of the system. Trust calculated as:

$$T_k = \frac{\sum_1^n t_{ik}}{n}, \; 1 \le k \le n \tag{1}$$

Here n number of system offers the cloud services and, T_k is the total trust value of the system k. Also, i times the transactional history is available with the system. After calculating the T_k value, it is compared against the threshold value, say, 85%. If the T_k value lies in the range of tier-1, the system is considered for next transaction and the credentials are updated for current transaction. If the T_k value lies in tier-2, the system is marked for consideration. Here, the tier-2 systems are backup systems reserved for tier-1 level's failure or shall be considered for second level assignment. Second level assignment means

are to be considered, if no systems are available in tier-1. Tier-3 and tier-4 systems shall be marked as untrusted systems. Several approaches like[4], penalize the systems in tier-3 and tier-4 according the aggregate values, to ensure systems not participating with old credentials in next iteration. Thus, on the next iteration tier-3 and tier-4 systems are avoided from participating.

3.1.2 Indirect Method

In direct method trust value can be calculated only if the system has the transactional history with the service provider. In several instances cloud users may not have any transactional history with the cloud service provider. In these instances system with transactional history over service providers are considered. With additional conditions in[3,4,6] apart from trust calculation, reputation of the recommender system is evaluated. Since the external system is used; the feedback credibility in terms of reputation of the system must be evaluated first. Different approaches do available to evaluate the feedback credibility of the system. Filtering the recommenders is carried in different ways. One hop relationship is a method that considers the direct relationship with the service provider and is better preferred than other methods. In other words systems with direct interactions are alone considered as recommender system. While the methods for securing the trust calculations are provided[9–11] it is beyond applying the trust calculation for evaluating the feedback credibility.

3.2 Framework Methods

Framework methods are categorized in two types, systems with trust value calculation and without calculation for evaluation. Calculation based methods needs data maintenance by the user for establishing the trust between user and service provider. Certainly methods involving calculations and data maintenance by the user faces either or both the problem of time and space complexity. A framework based method avoids time and space complexities at the user end against certain demerits. In spite of the demerits of framework based methods, there are few decent works like[6,12–14] to evaluate trustworthiness of resources.

3.2.1 Qualitative Methods

Methods with calculations for trust estimation are almost like feedback based methods of trust estimation. Unlike the previous methods users need not calculate trust value instead; third party like systems will carry the calculations on behalf of the users. Like in[6], all the calculations are using the feedback methods (direct and indirect). Credibility of the resources and users can be estimated by feedback collection and assessment of the systems out of the actual system. In general the complete system is contained in a framework.

3.2.2 Quantitative Methods

Methods without calculations like[12–14] saves time by not involving complex calculations. In general, approaches to quantitatively establish trust in cloud environment falls under any one of the following category:

- Agent Based.
- Log Based.
- Authentication Based.

3.2.2.1 Agent Based Trust

Agents are deployed to assess and access the cloud services. Cloud service providers may not interact with end users until the commencement of the services, agents establish the communication after the potential users and providers are mapped with each other. Different purposes are satisfied by deploying agents, for instance an agent intended for identifying availability may list all the available resources from providers end currently. Agents are also deployed to update the trust value and their current status. Agents may interact with a single service provider to assess its various metrics like availability, integrity, confidentiality, data etc. In this scenario as mentioned in Figure 1 several agents may be deployed to assess and update the user's queries.

Agents are also used to identify different cloud providers for a single required service. As mentioned in Figure 2 several cloud service providers are identified by several agents deployed. In this scenario, as depicted in Figure 2, a cloud user may access multiple services from different service providers; an agent makes it transparent to the users. Here, the use of multiple agents also increases the reliability of the services accessed.

3.2.2.2 Log Based Trust

Log based methods establishes trust from the evidences obtained from the log files available from the target

systems. Event logs are collected in a secure manner to evaluate the worthiness of the system activities. Analyzing the logs reveal the suspicious activities of the target system. On the other hand various strengths of the system like down time, recovery time, up time, availability and attestation of entities are also obtained. Log mechanisms are also used to verify the attested entities. Attestation time stamps are used to verify the time validity of the stampings. In practice logs are hard to be accessed which is considered to be the serious set back of this approach.

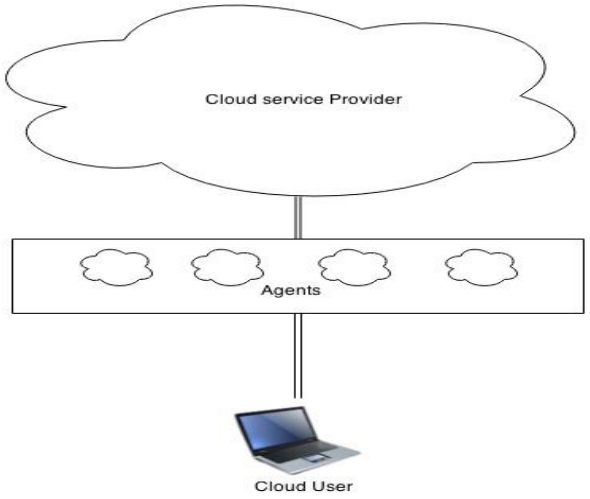

Figure 1. Agent's interaction with a service provider.

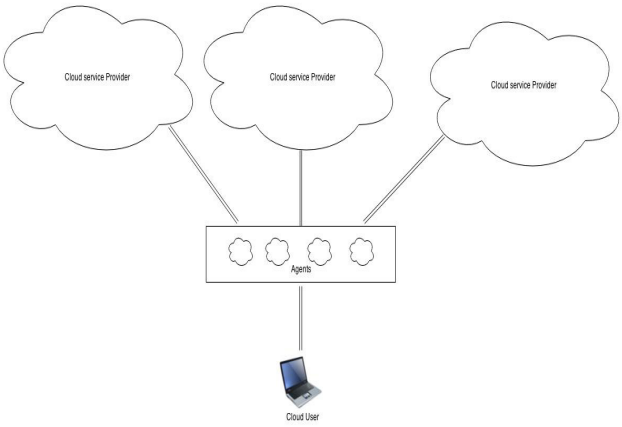

Figure 2. Agent's interaction with multiple service providers.

3.2.2.3 Authentication Based Method

In authentication based trust methods for cloud computing, message authentication is used preferably over other types of authentication. Normal authentication process metrics like private and public keys are used to communicate internally and externally. Internal resources and external resources are to be scrutinized for trust worthiness. Internal resources are used within datacenter's and are largely controlled by administrators. External resources or outsourced resources are unable to be controlled by internal administrators, due to cross domain policies. Thus, message authentication gives us an enormous support to control the resources outsourced to be controlled from actual source resources. This authentication approach shall be employed over cross domain policies too. Internal communication can also be encrypted and authenticated from unintended recipients.

Figure 3 denotes sequence of events triggered between various participating objects over trust establishment process by means of message authentication. Step 4 in Figure 3 indicates transfer of credentials from service provider to cloud user. Some credentials include private key, public key, log details, trust value, reputation ratings etc.

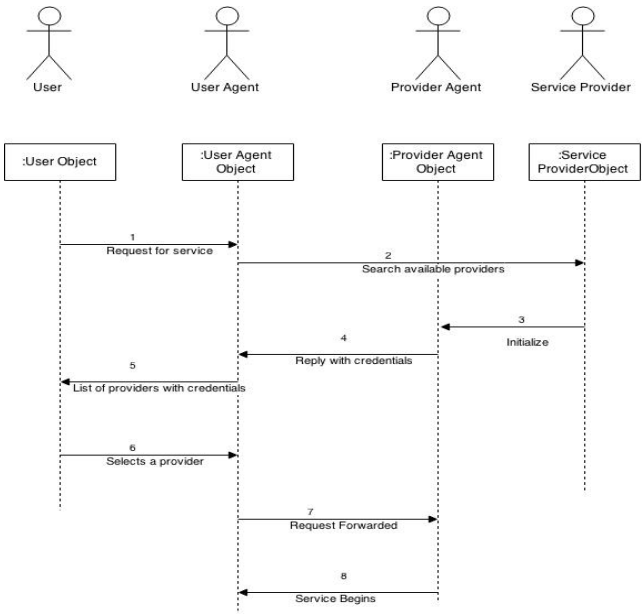

Figure 3. Sequence diagram of authentication based trust.

3.3 Attribute Based Trust

So far all the methods discussed collect the feedback from prior interaction or fixes a framework to make sure the workflow of the processes are aligned within the manageable boundary. Here in attribute based method, instead of collecting the complete interaction history, user end concentrates on several key attributes to be monitored. In[15] attributes are assigned some weights based on the preferential metrics. On successful or failure interaction with

the specific provider adjustments are made to the subsequent attributes weights. Calculation of the weights and subsequent trust values are based on feedback methods. Methods are almost similar for estimating the trust values as mentioned in the previous section.

In another type of attribute based trust, data provenance is used as the trust metric for estimating the trustworthiness of the service provider. In[16] a new method was proposed to secure the access control through the origin of data, rather considering the data from the feedback process. The data provenance method has the additional task of verifying the service provider's integrity as like the reputation systems. Even though task of identifying the integrity of the data may sounds complex, it helps to sort out the problem of misleading data from the feedback process. Thus the data and the owner of the data decide the trustworthiness of the information shared. Hence, attributes to be considered carefully on the feedback process for estimating the trustworthiness.

3.4 Protocols

Provision for the users to enquire about the transparency of the services being offered will make cloud more trustworthy. This provision of transparency is proposed through a protocol in[17] and the same was supported in[18]. The protocol will help not only the cloud user but also the service provider. Still improvements are being carried in setting up a sturdy standard for a protocol, in its present form called as CTP 2.0 (CloudTrust Protocol).

4. Ongoing Work and Conclusion

Several researches[19,20] are in progress globally to address and eradicate the trust barricades in cloud environment. To begin with feedback model provides excellent view about the service provider's trustworthiness. Direct method of feedback model needs past transactional history over the estimating provider. Indirect method overcomes the draw back of the need of transactional history. Still the domains like context specificity. i.e. type of service provided needs to be greatly addressed. The major setback of feedback model is the prior of experience of transaction with the specific service provider. Problem aggravates when a provider changes the behavior on current transaction unexpectedly. The concern is yet to be addressed. Also need to collaborate with other users becomes vital, which may give raise to the chance of malicious recommenders.

Ongoing research in establishing the clear frame work towards the services being provisioned is the welcome move. A frame work method has the capability to address the issue easily but it is in the incubation stage. Architecturally string frameworks must be evolved to fit it into any of the system and shall be used as open architecture across cloud too.

Quantitative and qualitative methods may help us to serve better. While qualitative methods involve complex computation like in feedback methods, carries the limitations of the prior method too. Log based quantitative methods needs to look into the log activities of internal and external system. Has the demerits of recursive search within a log, file corruption and modification are also possible. Complexity multiplies for log maintenance for frequent interaction. Dedicated space for the log activities is another concern. Agents based methods has the problem of traditional problem in agents approaches. Two tier trust check is to be in place in agent based approach. First check is against the trustworthiness of the agents and then the trustworthiness of the concerned system.

In general, the methods discussed in the previous section are the primitive steps to make cloud users to believe cloud a trustworthy as traditional services. This study reveals the gap between the actual barricades to Cloud Computing and the proposed methods. Solution to the problem of cloud trust states that on successful transaction of the entities with a service provider, one can evaluate the trustworthiness of the service provider. At the same time cloud is dynamic and hence needs sophisticated approaches to solve the problem of cloud trust dynamism. More firm mathematical models are required to express the trust, which is still open in any distributed environment. Hence, the problem of trust in Cloud Computing is wide open still. In future some of the cloud forums may be expected to solve the problem of cloud trust. Cloud Security Alliance (CSA) CloudTrust Protocol 2.0 may be promising the future cloud trends.

Once cloud services are adopted in full swing, resource utilization can be attained to the maximum level thereby cost of IT operations shall be greatly be reduced.

5. Acknowledgements

Authors would like to extend heartfelt thanks to ACRF (Anna Centenary Research Fellowship) and Parul University for the continuous financial support for this research work.

6. References

1. Coles C, Yeoh J. Cloud adoption practices and priorities survey report. Cloud Security Alliance; 2015 Jan.
2. Cloud Usage: Risks and opportunities report. Cloud Security Alliance (CSA); 2014 Sep.
3. Zhu C, Nicanfar H, Leung VC, Yang LT. An authenticated trust and reputation calculation and management system for cloud and sensor networks integration. IEEE Transactions on Information Forensics and Security. 2015 Jan; 10(1):118–31.
4. Gokulnath K, Uthariaraj VR. Fair-trust Evaluation Approach (F-TEA) for cloud environment. International Symposium on Security in Computing and Communication; Springer Berlin Heidelberg; 2014 Sep. p. 81–91.
5. Lin Guoyuan L, Wang Danrul W, Yuyul B, Min L. MTBAC: A Mutual Trust Based Access Control Model in Cloud Computing. China Communications, Informations Security; 2014 Apr.
6. Noor TH, Sheng QZ, Trust as a service: A framework for trust management in cloud environments. Springer-Verlag Berlin Heidelberg, WISE 2011, LNCS 6997; 2011. p. 314–21.
7. Shen H, Liu G. An efficient and trustworthy resource sharing platform for collaborative cloud computing. IEEE Transactions on Parallel and Distributed Systems. 2014 Apr; 25(4):862–75.
8. Sato H, Kanai A, Tanimoto S. A cloud trust model in a security aware cloud. 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT); 2010 Jul. p. 121–4.
9. Chong SK, Abawajy J, Ahmad M, Hamid IR. Enhancing trust management in cloud environment. Procedia-Social and Behavioral Sciences. 2014 May; 129:314–21.
10. Article title. 2016. Available from: http://www.emc.com/emc-plus/rsa-thought-leadership/cloud/cloud-trust-authority.html
11. Wu X, Zhang R, Zeng B, Zhou S. A trust evaluation model for cloud computing. Procedia Computer Science. 2013 Dec; 17:1170–7.
12. Abbadi IM, Alawneh M. A framework for establishing trust in the Cloud. Elsevier, Computers and Electrical Engineering. 2012; 38(5):1073–87.
13. Ko RKL, Jagadramana P, Mowbray M, Pearson S, Kirchberg M, Liang Q, Lee BS. Trust Cloud: A framework for accountability and trust in cloud computing. IEEE ICFP; 2011.
14. Talib AM, Atan R, Abdullah R, Murad MAA. Towards a comprehensive security framework of cloud data storage based on multi-agent system architecture. Journal of Information Security. 2012; 3:295–306.
15. Li X, Du J. Adaptive and attribute-based trust model for servicelevel agreement guarantee in cloud computing. IET Inf Secur. 2013; 7(1):39–50.
16. Bertino E, et al. A roadmap for privacy-enhanced secure data provenance. Journal of Information system. NewYork: Springer Science Business Media; 2014.
17. Knode R, Egan D. Digital trust in the cloud: A Precis on the cloud Trust Protocol (V2.0). CSC; 2010 Jul.
18. Knode R. Cloud trust protocol orientation and status. Cloud Security Alliance; 2011 Jun.
19. Dutta P, Kumaravel A. A novel approach to trust based identification of leaders in social networks. Indian Journal of Science and Technology. 2016 Mar; 9(10).
20. Khan KM, Malluhi Q. Establishing trust in cloud computing. IT Professional. 2010 Sep; 12(5):20–7.