International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 3; Issue 5; September 2018; Page No. 01-06

Service based trust and reputation of cloud and wireless sensor networks

Tanuja R[1*], Sukanya Thapa[2], Manjula SH[3], Venugopal KR[4]
[1-4] University Visvesvaraya College of Engineering, Bangalore University, Bangalore, Karnataka, India

Abstract
The integration of a Wireless Sensor Network which consists of a large number of low-cost, low-power, multifunctional and resource-constrained sensor nodes with cloud computing which is featured by powerful data storage and data processing capabilities, has become an important area of research in today's technology driven world. The efficient utilization of cloud computing and wireless sensor networks integrated system demands transparency into the trustworthiness of the service provider. Existing works, compute trust and reputation of a service provider for every service it offers for each service user. This infers when a service user needs to choose the most trustworthy service provider, it considers only the past experience of itself with different service providers which may or may not result in selection of a service provider from a set of service provider which may be bad, good or average. The proposed work provides better visibility into the trustworthiness of a service provider by considering past experience of all the service users for a service from a service provider to conclude its trustworthiness. This results in high probability of selection of a trustworthy service provider by the service user for a service which would eventually lead to their satisfaction and would make their investment into service worth.

Keywords: cloud services, reputation, trust, reliable service, wireless sensor networks

1. Introduction
A wireless sensor network consists of spatially distributed autonomous sensors which monitor physical or environmental conditions (eg temperature, sound, pressure) and cooperatively pass their data through the network to a central location where data undergoes processing and gets transmitted to their point of application. The development of wireless sensor networks has its roots in military applications such as battlefield surveillance. Since then such networks have found application in health care monitoring, Environmental/Earth sensing (e.g. Air pollution monitoring, Forest fire detection, Landslide detection) Industrial monitoring (e.g. Machine health monitoring, Data logging, Water/Waste water monitoring, Structural Health Monitoring) [1].

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]. Cloud Computing model provides several benefits such as on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service by making the services available in various forms such as Software as a Service(SaaS), Platform as a Service(PaaS), Infrastructure as a Service(IaaS). The cloud infrastructure and services can be provisioned by deployment of models such as Private cloud, Community Cloud, Public Cloud and Hybrid Cloud.

The idea of integration of a Wireless Sensor Network (WSN), which consists of a large number of low-cost, low-power, multifunctional and resource-constrained sensor nodes with cloud computing featured by powerful data storage and data processing capabilities, has become an important area of research in today's technology driven world [3-5]. Fig.1 shows an example of a cc-wsn integrated system where sensor network providers (SNPs) provide the sensory data (e.g., traffic, video, weather, humidity and temperature) collected by deployed WSNs to the cloud service providers (CSPs). CSPs utilize the powerful cloud to store and process the sensory data and then further on demand offer the processed sensory data to the cloud service users (CSUs).

The motivation of the work is due to the integrated system of cloud and sensor networks. CSUs and CSPs need to have a mechanism on which they can rely to choose a trustworthy CSP and SNP respectively, without which there is high probability that a CSU or CSP could select an untrustworthy CSP or SNP and end up getting a poor service. There exist systems like ATRCM [13] which provides a mechanism to choose a reliable service provider based on trust and reputation calculated from the feedback of service users. This existing system suffers from a drawback, it maintains a trust value of each service from each service provider to each service user and so the service user makes a choice of reliable service provider based on the history of its own experience with the service providers. The selection criteria may result in the selection of a service provider from a set of service providers which may be good or average or bad as the trust value considers only the experience of the service user asking for the service. This issue is addressed in this paper and an enhancement is suggested which would help the service users to have more transparency in terms of trust and reputation while choosing the service provider.

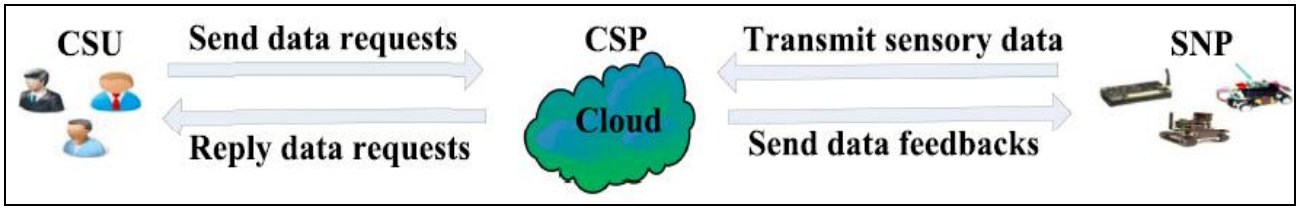

Fig 1: Schematic diagram of a cc-wsn integrated system

The main contribution of this paper is that an enhancement has been proposed over the existing systems which would make the selection a trustworthy service provider more transparent. According to the proposal, the feedback of each service user for each service from each service provider would be considered to calculate the trust and reputation of that service provider. So the system would have the feedback from each CSU for a particular service from a CSP would be considered to calculate the trust value of the corresponding CSP and also, the feedback from each CSP for a particular service from a SNP would be considered to calculate the trust value of the corresponding SNP. This would bring more transparency into the system and provide better visibility into the trust and reputation of services being offered. As the past experience of every CSU and every CSP is brought into the calculation of trust and reputation of each service of a particular CSP and SNP respectively, a CSU and a CSP can easily select the most trustworthy and reputed CSP with less efforts.

The rest of the paper is organized as follows. Section 2 introduces the related work and Section 3 provides background for our paper and proposed solution. Section 4 presents preliminaries and Section 5 presents problem definition and algorithm. Section 6 provides performance analysis and finally section 7 gives conclusion of the paper.\

2. Related work

This section presents the current works on trust and calculation in CC-WSN integrated system.Work in [6] suggests application of a trust-overlay network over multiple data centers to implement reputation system to establish trust between service providers and data owners where data coloring and software watermarking techniques protect shared data objects and massively distributed software modules and these techniques safeguard multi-way authentications, enable single sign-on in the cloud, and tighten access control for sensitive data in both public and private clouds. [7] Suggests enabling indirect mutual trust between the owner and the Cloud service providers (CSPs) which offers Storage-as-a-service. Continuous on trust attributes owing to the dynamic nature of the cloud to enforce service-level agreements has been suggested in [8] and presents an adaptive trust management model monitoring for efficiently evaluating the competence ofa cloud service based on its multiple trust attributes. A proposal of a framework to examine trust of cloud resources by an armor which constantly monitors and assesses the system and checks the resources which armor protects is demonstrated in [9]. A trust model to gather and analyze the reliability of cloud resources based on the historical information of servers for efficient reconfiguration and allocation of cloud computing resources is proposed in [10, 11], a framework of trust as service has been proposed to improve current trust managements by introduction of an adaptive credibility model to distinguish the credible and malicious feedbacks. The work of [12] presents effectively using trust management to enhance the security of a cloud integrated WSN system. Work presented in [13], trust system named as ATRCM [13] is the first work calculating and managing the trust and reputation in the scenario of integrating CC and WSNs by taking authentication of service providers into account. Our proposal makes a trust based system transparent for the service users which are cloud service users taking service from cloud service provider and cloud service providers taking service from sensor network providers, by providing them better visibility into the trust and reputation of each service of the service providers.

3. Background

The existing system ATRCM [13] is the first research work which incorporates authentication of service users and service providers with trust and reputation management of service providers. It introduces an entity named TCE which computes the trust and reputation values and manages them. The system lets service users authenticates service providers to avoid malicious impersonation attacks by verifying certificate provided by them. The system calculates and manages trust and reputation regarding the service of service providers and helps service users choose desirable service provider by filtering them based on their attributes and, trust and reputation values. It uses beta distribution to map the feedback provided by service users to trust and reputation values [14, 16] illustrated as follows. Let S and F represent the (collective) amount of positive and negative feedbacks provided by service users about a service, then the trustworthiness T of that service provider is computed as $T=(S+1)/(S+F+2)$.

Based on the feedbacks of previous services, if a service user chose the service of a service provider, then it means that the service user somehow trusted that service provider and decided to use the service of it. Its assumed that the number of service users that chose the service of the service provider is N and the number of service users that needed the service to receive from a service provider is N'($N' \leq$ total no of service users). Then the reputation value R of the service of the service user is calculated by R = N/N'. The trust and reputation calculation mechanism of the ATRCM [13] system is cumbersome as trust and reputation value needs to be calculated for each combination of CSU, CSP and service type and CSP, SNP and service type. Also, mechanism involves comparison of CSU's and CSP's own experience history for a service with respect to different CSPs and SNPs respectively to select a CSP or SNP which is not an efficient and healthy method.

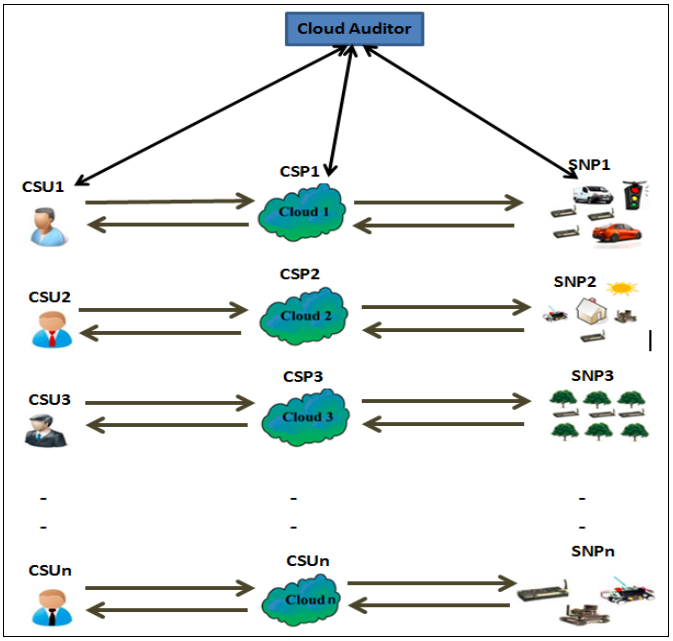

Fig 2: System overview of integrated cc-wsn netwo

4. Preliminaries

As shown in the Fig. 2, a CC-WSN system consists of multiple cloud service users (CSU), cloud service providers (CSP) and sensor network providers (SNP). The deployed WSNs sense and collect the data specific to their purpose (e.g., traffic, weather, temperature) andthe SNPs provide these sensory data to CSPs. The powerful clouds are utilized to store and process the sensory data and the CSPs offer the processed sensory data to the CSUs on demand. There exist an entity named cloud auditor which monitor the whole system by collecting feedback from service users about the service a service provider and computing trust and reputation values, and providing these values on demand to service users.

The service requests for sensory data by each CSU are assumed to possess following attributes: Data Type (DT), Data Size (DS), Data Request Speed (DRS), Data Service Time (DST) and Data Service Pay (DSP). The cloud services offered by each CSP are assumed to possess following attributes: Cloud Service Type (CST), Cloud Storage Size (CSS), Cloud Processing Speed (CPS), Cloud Operation Time (COT) and Cloud Service Charge (CSC).

The services of sensor network offered by each SNP is assumed to possess following attributes: Sensor Type (ST), Sensor Network Coverage (SNC), Sensor Network Throughput (SNT), Sensor Network Lifetime (SNL) and Sensor Network Service Charge (SNSC). There is a trust value (Tc) and a reputation value (Rc) associated with each service of a CSP and there is a trust value Tsand a reputation value (Rc) associated with each service of a SNP.Each CSU owns a minimum acceptable value of trust (Tcmin) and minimum acceptable value of reputation (Rcmin) for each service of a CSP. Each CSP owns a minimum acceptable value of trust (Tsmin) and minimum acceptable value of reputation (Rsmin) for each service of a CSP. There is a cost difference (Cc) between the CSC of CSP and DSP of CSU for each service (Cc = CSC – DSP). There is a cost difference (Ck) between the SNSC of SNP and SNSP of CSP for each service (Ck= SNSC – SNSP). Each CSU owns an acceptable range (Cbc) about Cc. In addition, each CSP owns an acceptable range (i.e., Cbk) about C. The interval of Cbc and Cbk are |Cbc| and |Cbk|, respectively. Each CSU has three weights (αc, βc and γc) in terms of the importance of Cost, Trust and Reputation, while αc + βc +γc = 1. Similarly, each CSP owns three weights (αs, βs, γs).

5. Problem definition and algorithm

In the existing system, there exists a trust value of each service from each service user to each service provider.This implies that there exist a trust value of each service from each CSP to each CSU and also there is a trust value of each service from each SNP to each CSP. The trust value of a particular service of each CSP for a CSU is compared with the minimum acceptable value of the trust for that service and hence usatisfying CSPs are filtered out. Similarly, the trust value of a particular service of each SNP for a CSP is compared with the minimum acceptable value of the trust for that service and hence usatisfying SNPs are filtered out. The existing system calculates trust for every combination of CSU, CSP and Service type and also, for every combination of CSP, SNP and service type and can be observed from Fig 3. The drawback here is that, it maintains a trust value for each service from each service provider to each service user and so the service user makes a choice of reliable service provider based on the history of its own experience with the service providers. The selection criteria may result in the selection of a best service provider from a set of all bad service providers as the trust value considers only the experience of the service user asking for the service. In the existing system, there exists a trust value of each service from each service user to each service provider. This implies that there exist a trust value of each service from each CSP to each CSU and also there is a trust value of each service from each SNP to each CSP. The trust value of a particular service of each CSP for a CSU is compared with the minimum acceptable value of the trust for that service and hence unsatisfying CSPs are filtered out. Similarly, the trust value of a particular service of each SNP for a CSP is compared with the minimum acceptable value of the trust for that service and hence unsatisfying SNPs are filtered out. The existing system calculates trust for every combination of CSU, CSP and Service type and also, for every combination of CSP, SNP and service type and can be observed from Fig 3. The drawback is it maintains a trust Value for each service from each service provider to each service user and so the service user makes a choice of reliable service provider based on the history of its own experience with the service providers. The selection criteria may result in the selection of a best service provider from a set of all bad service providers as the trust value considers only the experience of the service user asking for the service.

The proposed enhancement is that the feedback from each service user for a service would be considered to compute the trust and reputation for the corresponding CSP for that service. This infers that feedback from each CSU for a particular service from a CSP would be considered to calculate the trust value of the corresponding CSP and also, the feedback from each CSP for a particular service from a SNP would be considered to calculate the trust value of the

corresponding SNP. This would bring more transparency into the system and provide better visibilty into the trust and reputation of services being offered. As the past experience of every CSU and every CSP is brought into the calculation of trust and reputation of each service of a particular CSP and SNP respectively, a CSU and a CSP can easily select the most trustworthy and reputed CSP with less efforts.
Algorithm consists of phases like (i) Cloud preprocessing phase, and (ii) User processing phase.

1. Cloud preprocessing phase: In this phase cloud auditor executes the following steps

Feedback collection
Auditing whether received feedbacks that are to be utilized to calculate trust and reputation are genuine, by security audit, privacy impact audit and performance audit, and etc.

Calculation of trust
Let *n* be the possible number of Cloud Service Types and a CSP can offer less or equal number of these services then consider CS Tset = $\{CST_1, CST_2 ..... CST_n\}$ be the set of *n* cloud services, and T cset = $\{T_1, T_2 ..... T_n\}$ be the set of corresponding trust values and R cset = $\{R_1, R_2 ..... R_n\}$ be the set of corresponding reputation values.
Let m be the possible number of Sensor Types and a SNP can offer less or equal number of sensory data from these sensor types as services then consider STset = $\{ST1, ST_2 ..... ST_m\}$ be the set of *m* sensor types, and Tsset = $\{T_1, T_2 ..... T_m\}$ be the set of corresponding trust values and Rsset = $\{R_1, R_2 ..... R_m\}$ be the set of corresponding reputation values.
Consider x number of Cloud service users used the same service CST_i.
If CSU_q has used this service p_q times, out of which k_q times it has been successful.

$$S_i = k_1 + k_2 + \ldots\ldots\ldots + k_x = \sum_{q=1}^{x} (k_q)$$

$$F_i = (p_1 - k_1) + (p_2 - k_2) + \ldots\ldots\ldots + (p_x - k_x) = \sum_{q=1}^{x} (p_q - k_q)$$

$$T_i = \frac{S_i + 1}{S_i + F_n + 2}$$

Calculation of reputation
Let CN_c be the number of CSUs that chose the service of the CSP and N'_u ($N'_u \leq N_u$) be the number of CSUs that needed the service to receive from a CSP.

$$R_i = \frac{CN_c}{N'_u}$$

2. User processing phase
CSU-CSP service request processing
A CSU executes following filtering steps to select a CSP for its service requirement
Filter 1: CSU filters the suitable CSPs by comparing its attribute requirement with attribute of CSPs.
$CST \supseteq DT$
$CSS \geq DS$
$CPS \geq DRS$
$COT \geq DST$

Filter 2: On request CSU gets T_c value of the required service of the filtered CSPs (from Filter 1) from cloud auditor. CSU further filters the CSPs by comparing T_c with T_{cmin} value.
$T_c \geq T_{cmin}$
Filter 3: On request CSU gets $R_c$value of the required service of the filtered CSPs (from filter 2) from cloud auditor. CSU further filters the CSPs by comparing R_c with R_{cmin} value.
Filter 4: CSU further filters the CSPs by checking if Cc value is within Cbc which is the difference between CSC of CSP and DSP of CSU.
$C_c \in Cb_c$
Filter 5: CSU chooses the service offered by the CSP with the maximum M_c [16] and informs cloud auditor about signed SLA or PLA.

$$M_c = -\alpha_c \cdot \frac{Cc}{|Cbc|} + \beta_c \cdot T_c + \gamma_c \cdot R_c$$

CSU sends feedbacks about the service of the CSP to cloud auditor based on PLA and SLA after the termination of service. Cloud auditor stores and updates the T_c value as well as the R_c value.

CSP-SNP service request processing
A CSU executes following filtering steps to select a CSP for its service requirement

Filter 1: CSP filters the suitable SNPs by comparing its attribute requirement with attribute of SNPs. Also CSP checks if the attribute requirement of CSU offered by the SNPs.
$ST \supseteq DT$
$SNC \supseteq DS$
$SNT \geq DRS$
$SNL \geq DST$
$CST \supseteq ST$
$CSS \geq SNC$
$CPS \geq SNT$
$COT \geq SNL$

Filter 2: On request CSP gets T_s value of the required service of the filtered SNPs (from Filter 1) from cloud auditor. CSP further filters the SNPs by comparing T_s with T_{smin} value.
$T_s \geq T_{smin}$
Filter 3: On request CSP gets R_s value of the required service of the filtered SNPs (from filter 2) from cloud auditor. CSP further filters the SNPs by comparing R_s with R_{smin} value.
Filter 4: CSP further filters the SNPs by checking if C_s value is within Cb_s which is the difference between SNSC of SNP and SNSP of CSP.
$C_s \in Cb_s$
Filter 5: CSP chooses the service offered by the SNP with the

maximum M_s [16] and informs auditor about signed SLA or PLA.

$$M_s = -\bar{\alpha_s} \cdot \frac{Cs}{|Cbs|} + \beta_s \cdot T_s + \gamma_s \cdot R_s$$

CSP sends feedbacks about the service of the SNP to cloud Auditor based on PLA and SLA after the termination of service. Cloud auditor stores and updates the T_s value as well as the R_s value.

6. Performance analysis

In this section, we evaluate and compare the results of our proposed system with the existing system. Calculation of trust and reputation is based on the feedback given by CSUs and CSPs after usage of a service as per the steps given in the algorithm proposed. In the experiment performed, the cc-wsn system is assumed to consist of three CSUs, four CSPs and five SNPs. With the filter process of the user processing phase of algorithm proposed, we assume that three CSP and three SNPs are filtered as their attributes satisfy the requirements. The result of computation of trust and reputation value from the feedback of CS Ufor service CST1in the existing system and in our proposed system is tabulated in figure 4 and figure 6 respectively.

In figure 4, it can be observed that trust value and reputation value is considered for each CSU, each filtered CSP for service CST_1whereas from Table 3, it can be observed that

Table 1: Trust and Reputation values of CSU and qualified CSPs

	T_{cu}	R_c	T_{scu}	R_{sc}
$CSU_1 \leftrightarrow CSP_1 \leftrightarrow CST_1$	0.7	0.8	0.5	0.5
$CSU_1 \leftrightarrow CSP_2 \leftrightarrow CST_1$	0.8	0.7	0.5	0.5
$CSU_1 \leftrightarrow CSP_3 \leftrightarrow CST_1$	0.9	0.6	0.5	0.5
$CSU_2 \leftrightarrow CSP_1 \leftrightarrow CST_1$	0.7	0.8	0.5	0.5
$CSU_2 \leftrightarrow CSP_2 \leftrightarrow CST_1$	0.8	0.7	0.5	0.5
$CSU_2 \leftrightarrow CSP_3 \leftrightarrow CST_1$	0.9	0.6	0.5	0.5
$CSU_3 \leftrightarrow CSP_1 \leftrightarrow CST_1$	0.7	0.8	0.5	0.5
$CSU_3 \leftrightarrow CSP_2 \leftrightarrow CST_1$	0.8	0.7	0.5	0.5
$CSU_3 \leftrightarrow CSP_3 \leftrightarrow CST_1$	0.9	0.6	0.5	0.5

The cumulative trust value is considered from feedback of all the CSUswhich used the service in past. Similarly, the result of computation of trust and reputation values from the feedback of CSP for service ST_1 in the existing system and in our proposed system is tabulated in figure 5 and figure 7 respectively. In Table 7, it can be observed that trust value and reputation value is considered for each CSP, each filtered SNP for serviceST_1whereas from Table 4, it can be observed that the cumulative trust value is considered from feedback of all the CSPs which used the service in past

Table 2: Trust and Reputation values of CSP and qualified SNPs

	T_{cu}	R_c	T_{scu}	R_{sc}
$CSP_1 \leftrightarrow SNP_1 \leftrightarrow ST_1$	0.8	0.7	0.5	0.5
$CSP_1 \leftrightarrow SNP_2 \leftrightarrow ST_1$	0.7	0.6	0.5	0.5
$CSP_1 \leftrightarrow SNP_3 \leftrightarrow ST_1$	0.6	0.5	0.5	0.5
$CSP_2 \leftrightarrow SNP_1 \leftrightarrow ST_1$	0.8	0.7	0.5	0.5
$CSP_2 \leftrightarrow SNP_2 \leftrightarrow ST_1$	0.7	0.6	0.5	0.5
$CSP_2 \leftrightarrow SNP_3 \leftrightarrow ST_1$	0.6	0.5	0.5	0.5
$CSU_3 \leftrightarrow SNP_1 \leftrightarrow ST_1$	0.8	0.7	0.5	0.5
$CSU_3 \leftrightarrow SNP_2 \leftrightarrow ST_1$	0.7	0.6	0.5	0.5
$CSU_3 \leftrightarrow SNP_3 \leftrightarrow ST_1$	0.6	0.5	0.5	0.5

Table 3: Trust and Reputation of filtered CSPs

	T_c	R_c	T_{cmin}	R_{cmin}
$CSP_1 \leftrightarrow CST_1$	0.7	0.8	0.5	0.5
$CSP_2 \leftrightarrow CST_2$	0.8	0.7	0.5	0.5
$CSP_3 \leftrightarrow CST_3$	0.9	0.6	0.5	0.5

Table 4: Trust and Reputation of filtered SNPs

	T_s	R_s	T_{smin}	R_{smin}
$SNP_1 \leftrightarrow ST_1$	0.7	0.8	0.5	0.5
$SNP_2 \leftrightarrow ST_2$	0.8	0.7	0.5	0.5
$SNP_3 \leftrightarrow ST_3$	0.9	0.6	0.5	0.5

The management of the trust and reputation of the system in the improvised system is better as only a single trust and reputation value is associated with respect to each service offered by a service provider. In the improvised ATRCM [13], since the past experiences of all the Service Users who used particular service from a Service provider have been considered to compute the trust and reputation of the service provider, it gives a better visibility into the trustworthiness of a service provider and results in selection of most satisfactory service Provider. But in the original ATRCM [13], only the past experience of a CSU is used to calculate the trust for a service and hence may lead to selection of an untrustworthy service provider each time.

7. Conclusions

In this paper, we have proposed trust and reputation calculation mechanism of the Cloud and WSN system which considers past experience of all the CSUs who used a particular cloud service from a CSP and of all CSPs who have used a particular sensor service from a SNP, to compute the trustworthiness of that CSP and SNP respectively. This mechanism makes the system transparent for the service users and provides better a visibility into the trust and reputation values of service Provider. This would result in high probability of selection of a trustworthy service provider by the service user for a service which would eventually lead to their satisfaction and would make their investment into service worth.

8. References

1. Akyildiz F, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: A survey, Comput. Netw, Int. J Comput. Telecommun. Netw. 2002; 38(4):393-422.
2. Peter Mell, Tim Grance. NIST Definition of Cloud Computing v15, Version 15, 2010.
3. Yuriyama M. Kushida T. Sensor-cloud infrastructure-Physicalsensor management with virtualized sensors on cloud computing, in Proc. 13th Int. Conf. Netw-Based Inf. Syst, 2010, 1-8.
4. Fortino G, Pathan M, Di, Fatta G. Body Cloud Integration of cloud computing and body sensor networks, in Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci., 2012, 851-856.
5. Takabe Y, Matsumoto K, Yamagiwa M, Uehara M. Proposed sensor network for living environments using

cloud computing, in Proc. 15th Int. Conf. Netw.-Based Inf. Syst, 2012, 838-843.
6. Hwang K, Li D. Trusted cloud computing with secure resources and data coloring, IEEE Internet Comput. 2010; 14(5):14-22.
7. Barsoum Hasan A. Enabling dynamic data and indirect mutual trust for cloud computing storage systems, IEEE Trans. Parallel Distrib. Syst. 2013; 24(12):2375-2385.
8. Li X, Du J. Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing, IET Inf. Secur. 2013; 7(1):39-50.
9. Kuehnhausen M, Frost VS, Minden GJ. Framework for assessing the trustworthiness of cloud resources, in Proc. IEEE Int. Multi-Discipl. Conf. Cognit. Methods Situation Awareness Decision Support, 2012, 142-145.
10. Kim H, Lee H, Kim W, Kim Y. A trust evaluation model for QoS guarantee in cloud systems, Int. J Grid Distrib. Comput. 2010; 3(1):1-9.
11. Noor TM, Sheng QZ. Trust as a service: A framework for trust management in cloud environments, in Proc. 12th Int. Conf. Web Inf. Syst. Eng, 2011, 314-321.
12. Savas O, Jin G, Deng J. Trust management in cloud-integrated wireless sensor networks, in Proc. Int. Conf. Collaboration Technol. Syst, 2013, 334-341.
13. Chunsheng Zhu, Hasen Nicanfar, Victor CM. Leung Laurence Yang T. n Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration, in IEEE Trans. Information Forensics and Security. 2015; 10(1):2015.
14. Josang Ismail R. The beta reputation system, in Proc. 15th Bled Electron. Commerce Conf, 2002, 324-337.
15. Ganeriwal S, Balzano LK, Srivastava MB. Reputation-based framework for high integrity sensor networks, ACM Trans. Sensor Netw. 2008; 4(3):15.
16. Qin H, Yu C, Leung Z. Shen C. Miao Towards a trust aware cognitive radio architecture, ACM SIGMOBILE Mobile Comput. Commun. Rev. 2009; 13(2):86-95.