ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 07, pp.34032-34036, July, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

AN ACCREDIT RELIABILITY AND REPUTATION CALCULATION AND MANAGEMENT SCHEME FOR CLOUD AND WIRELESS SENSOR NETWORKS ALLIANCE

***,[1]Chandu, T. and [2]Vanajakshi Devi, K.**

[1]Sree Vidyanikethan Engineering College (Autonomous), Tirupati
[2]Department of Computer Science, Yogananda Institute of Technology & Science, Tirupati

ARTICLE INFO

Article History:
Received 10th April, 2016
Received in revised form
19th May, 2016
Accepted 04th June, 2016
Published online 16th July, 2016

Key words:

Reliability, Reputation,
Authentication,
Wireless Sensor Networks,
Cloud Computing.

ABSTRACT

Cloud Computing (CC) deals with incorporations of Enormous data storages and its heavy data processing abilities whereas on the other hand pervasive data collection capabilities of Wireless Sensor Networks (WSN). The interactions and communication between the CC-WSN makes a huge difference in acquiring results and greatly reduces human effort thus receiving a lot of attention from industrial and academic purposes as it provides lot of computing services. However accreditation or authentication for reliable services, reputation calculation and managing of cloud and sensor networks are rarely addressed as Cloud Service Providers (CSP) and Sensor Network Providers (SNP) are least explored issues in CC-WSN integration. This paper intends to propose a novel approach to minimize risk and highly trustworthy with authenticated service of CSP and SNP's for resource sharing between them that provides efficient and uninterrupted services for Cloud Service User (CSU). The proposed system mainly focuses on resolving issues like Accrediting of CSP's and SNP's to avoid any malicious attacks that replicate the data, calculating and managing reliability and reputation of CSP's and SNP's and assisting CSU in choosing CSP; assisting CSP to select appropriate SNP for alliance. Thus issues like management and trust in resource sharing of CSP's are profoundly reduced to deliver service to CSU with minimal cost and high quality service.

Citation: Chandu, T. and Vanajakshi Devi, K. 2016. "An accredit reliability and reputation calculation and management scheme for cloud and wireless sensor networks alliance", *International Journal of Current Research*, 8, (07), 34032-34036.

INTRODUCTION

Resource sharing and computing has become transformed and modeled as delivering a traditional utility. As these very highly required and used services in today's technology, the user doesn't care or concerned about how the data is shared between CSP and SNP's or how the services are hosted, how the alliance between cloud services and sensor networks while accessing services based on their requirements. So, there might be high probability of impersonation attacks because of no accreditation, no trust or reliability can be ensured while providing services, can experience a lot of delay while accessing the required services, CSP and SNP's can be in compatible whilst trying to access the services.

Cloud Computing

Cloud computing is a cutting edge technology that enables flexible, on-demand network access for a shared pool of configurable computing resources like servers, storage, applications, networks and services that can be provided to the users with minimal administrative effort and service provider interaction. CC provides users with convenient usage of *Platforms*- OS and middleware services, *Infrastructure*-networks, servers and storages, *Softwares.* The main focus is to provide efficient, secure and reliable services not only cost efficient but also easy to maintain the service providers that can be enhances as per the user demand and web based easy access to ensure uninterrupted qualitative services.

Wireless Sensor Networks

Basically sensors are highly sophisticated devices that are used to frequently detect any change in physical property like temperature, BP, moisture, speed etc.., that can be converted into signal that can be measured electrically. These sensors that are spatially distributed in any specific region autonomously to monitor physical or environmental conditions to cooperatively send data through network to main server are known as Wireless Sensor Networks (WSN). WSN has a wide range of applications in areas like biodiversity, industries, civilian and

Corresponding author: Chandu, T.
Sree Vidyanikethan Engineering College (Autonomous), Tirupati

defense. WSN's have a capability of changing the way of connecting humans with the physical world like never before.

CC-WSN's Interconnection

As it is clear that the cloud has a tremendous capabilities of huge data storage and data processing, its alliance with WSN makes it more sophisticated and helps in reducing the human effort to a great extent. This innovative paradigm draws attention as it is very widely useful in both industrial and academic purposes. The basic theme of CC-WSN's integration is to provide efficient services to end user. Here the sensors detect the anomaly and converts into signals, sends data from their distributed network to cloud which can store enormous amount of data. Later process and supplies the data on user demand. Specifically, the sensory data (traffic, video, climate changes etc..,) from SNP's are gathered by WSN's to CSP's which stores that huge amount of data and processes the data. Then on demand of appropriate CSU's have access to their sensory data with just a simple client to access the cloud. Here SNP's act as data sources for CSP's and CSP's act as data providers for CSU's.

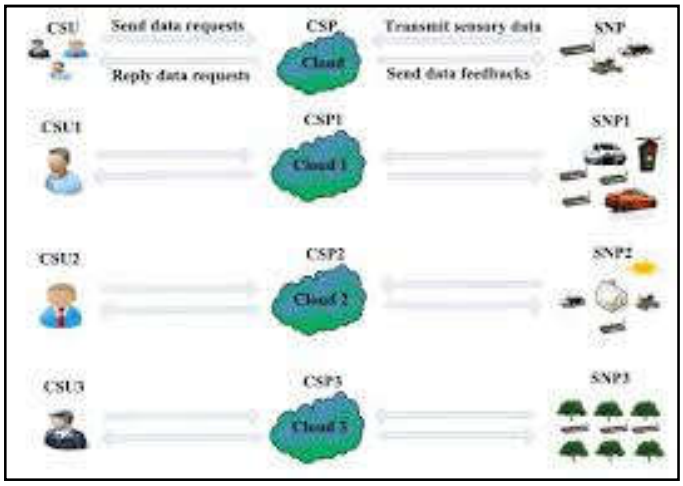


Fig.1. Alliance of CC-WSN

Research Motivation

In CC-WSN's integration, CSP's and SNP's are highly non explored issue should be taken into considered. However, this not only results in drastic results of CSU desirable service but also impedes a genuine SNP's sensory data to reach a CSP. *Accreditation of CSP's and SNP's:* There is a high probability of malicious attackers who can impersonate or fake our service while communicating between CSU's and CSP's and also between CSP's and SNP's. From thus fake SNP's and CSP's, CSU achieves mothing but loss of privacy or any delicate data. In addition to that, the reliability of the genuine SNP's and reputation of the CSP's are impaired by these fake SNP's and CSP's.

Trust and Reputation calculation and managing CSP's and SNP's: CSU may choose CSP with low trust and reputation without trust and reputation calculation of SNP's and CSP's. Then the desirable service of CSU may be fail to achieve reliable results or even experiences loss of data. On the other hand, CSP may also select an inappropriate or untrustworthy SNP's which may or may not provide the service desirable requested by CSP with large latency. To the best of our knowledge, the proposed system follows a novel approach to minimize risk and highly trustworthy with authenticated service of CSP and SNP's for resource sharing between them that provides efficient and uninterrupted services for Cloud Service User (CSU). The proposed system mainly focuses on resolving issues like Accrediting of CSP's and SNP's to avoid any malicious attacks that replicate the data, calculating and managing reliability and reputation of CSP's and SNP's and assisting CSU in choosing CSP; assisting CSP to select appropriate SNP for alliance. Thus issues like management and trust in resource sharing of CSP's are profoundly reduced to deliver service to CSU with minimal cost and high quality service.

Existed system

Since CC and WSN's are widely used technologies in areas like academia, industrial, development, research and defense that greatly reduces human effort to retrieve the desired data in required form. CC focuses on efficiency, security, privacy whereas WSN's focuses on reliability and accuracy. So, CC-WSN's integration results in heavy amount of study and research to compensate all these features along with operational cost. Verification in cloud has been improved a lot in recent years that aims at offering user friendly, mutual validation, identification of organization and meeting key agreement between cloud and the users. Regarding authorization CC-WSN incorporation, secure and extensible cloud planning scheme for sensor network system is planned in one of the operational system. It first describes the work and mechanism, then puts forward sanctuary mechanism for authorizing the users to retrieve sensory data, based on certificate authority based on digital signatures later replaced by Kerberos technique. The existing structure has its own bottlenecks such as: impersonated CSP's can communicate with CSU's by malicious attackers or fake to be reliable SNP's can be selected by CSP's. The trust and reputation of genuine CSP's and SNP's are also impaired by fake CSP's and SNP's. CSU's can't achieve anything useful from counterfeit CSP's and SNP's. In addition to that, CSU's may also experience delay in accessing information. Without trust and reputation computation and administration of CSP's and SNP's, leads CSU's to prefer for CSP's with low security and conviction. Moreover, CSP may just select any fake SNP that delivers unintended results with large latency.

Fig. 2. Existing CC-WSN Alliance

Proposed system

This paper proposes a novel accreditation for reliable and reputation computation and administrating for Cloud Computing and Wireless Sensor Networks alliance that signifies:

- Authorization of CSP and SNP
- Computing and managing reputation of SNP's and CSP's
- Reduces the delay in accessing the services and large latency in SNP's
- Instructing CSP to choose trustworthy CSP and assisting CSP to select an appropriate SNP to deliver desirable service.

Furthermore, we provide data owner with efficiently generated authenticator with encoding process simultaneously. This scheme is proven to be highly efficient, secure and the performance evaluation of this scheme makes this feasible to integrate with An Accredit Reliability and Reputation Calculation and Management Scheme for Cloud and wireless Sensor Networks Alliance. The most important element and key to our work is to enable and assist CSU in choosing authentic and desirable CSP as well as instructing CSP to select genuine SNP that delivers desirable service to the CSU. Hence we focus more on authorization of CSP and SNP rather than authentication of CSU. So, SNP and CSP are applied to certify by internationally recognized Information Security Management System (ISMS) standard by ISO. An SLA (Service Level Agreement) is a negotiated agreement between two or more parties, ion which one is the customer and the others are Cloud Service providers. SLA specifies the level of serviceability, performance, availability, operation and other parameters of the service. Usually, SLA addresses the segments about service: performance measurement, duties, problem management, warranties, definition, and termination. The result of the service received by the CSU is nothing but the subject of SLA. A PLA (Privacy Level Agreement) is also an agreement to describe how CSP maintains its level of privacy protection. The SLA between CSP and CSU provides specific attributes and minimum levels of other performance (e.g., cloud operations time, cloud processing speed) of CSP, while PLA address personal data protection and information privacy issues about cloud service.

Based on the five main roles (e.g., CSP, CSU, cloud broker, cloud carrier and cloud auditor) in this paper, we assume that cloud auditor is assigned to TCE. The fulfillment of service of the CSP is achieved when the CSP needs to receive and store the sensory data from appropriate SNP. Then the CSP process that huge amount of raw sensory data and made it accessible to CSU when demanded through their desirable service.

The various kinds of trust that we came across during this process (clod data processing trust, cloud data storage trust, cloud data transmission trust and cloud data privacy trust) which assists CSU in choosing the service of CSP. In this paper, the only trust that concerns CSU to choose the service of CSP are the three types (cloud data processing trust, cloud data transmission trust and cloud data privacy trust).

In the proposed scheme, the SNP's achieves the significant goals:

- Accrediting CSP and SNP to prevent impersonation of service by malicious attackers.
- Sequel payments on your analyzing and managing reputation and trust about the service of CSP and SNP
- Assisting CSU in choosing secure CSP and helping CSP to select appropriate SNP.

Efficiency of this system involves in improving: diverse security policies for several yet significant domains, the historical data of entity influences, transaction framework, and measurement of trust benefit dynamically considered by the unit, the trust model works with the firewall and does not really break the firewall's localized control policies.

Implementation

Accreditation flowchart of CSP and SNP

1. CSPs provide their certificate of authorization to CSU and CSU checks the signature of the certificate for validation and whether the certificate is revoked. Then CSU filters the CSPs that are not qualified.
2. SSPs provide their certificate of authorization to CSP and CSP checks the signature of the certificate for validation and whether the certificate is revoked. Then CSP filters the SNPs that are not qualified.

Reliability and Reputation calculation and Management between CSU and CSPs:

1. From the available CSPs, CSU checks whether the characteristics satisfy the attribute requirement of CSU. Filter the CSPs that are not satisfied.
2. CSU issues request to TCE and achieves trust value of service from CSP to CSU. Now CSU checks whether the trust value is greater than or equal to minimum trust value of service from CSP to CSU. Filter the CSP's that are not satisfied.

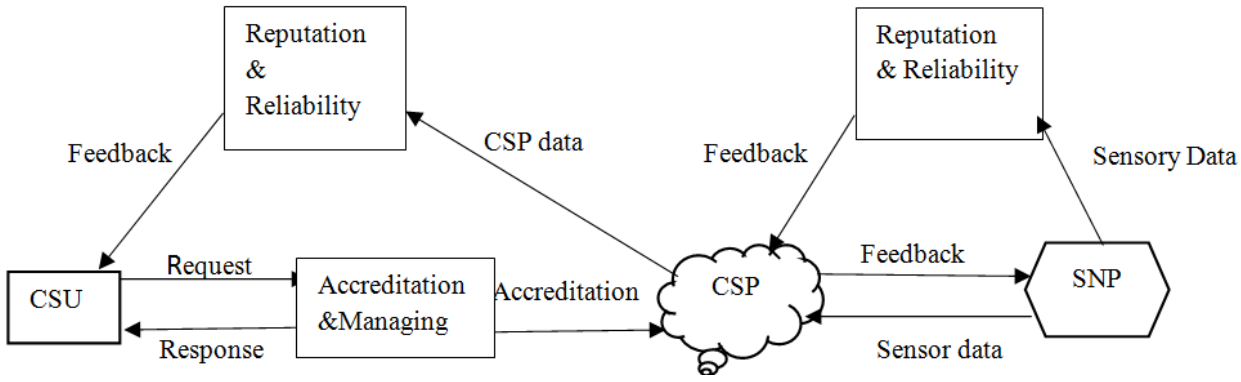


Fig. 3. System Architecture of Accrediting & Reputation Calculation & Management

3. Now CSU forwards its request to TCE and achieves the reputation value of service provided by CSP. CSU checks whether this value is greater than or equal to minimum acceptable reputation value of service by CSP. Filter CSP's that are not satisfied.
4. CSU calculates the Cost Service Charge value of CSP and Data Service Pay of CSU and checks whether the value lies within the acceptable range. Filter the CSPs that are not satisfied.
5. CSU checks whether Certificate of authorization of CSP is revoked and chooses the service offered by CSP with maximum trust and reputation value , informs TCE about signed SLA or PLA.
6. CSU sends feedbacks about service of CSP to TCE (Trusted Center Entity) based on PLA and SLA after the termination of service. TCE stores and updates the trust value as well as reputation value.

Trust and Reputation Calculation and Management between CSP's and SNP's:

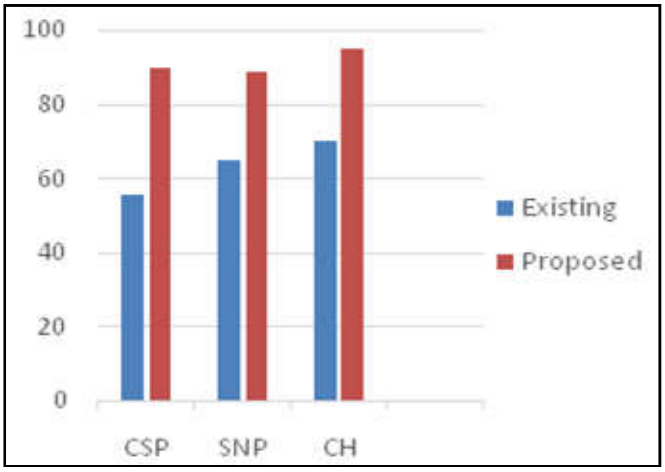
1. CSP checks whether the characteristics of SNP's satisfy the attribute requirement of CSP. CSP also checks whether the characteristics of SNP able to provide desirable service of CSU. Filter SNP's that are not satisfied.
2. CSP provides requests to TCE and receives the trust value of service from SNP to CSP. CSP then checks whether the value is more than or equal to the minimum acceptable value of service from SNP to CSP. Filter the SNPs that are not satisfied.
3. CSP issues requests to TCE and receives the reputation value of the service offered by the SNP. CSP checks whether this value is more than or equal to minimum acceptable reputation value of service. Filter the SNP's that are not qualified.
4. CSP computes Sensor Network Service Charge of SNP and Sensor Network Service Pay of CSP and checks whether this value lies within the acceptable range. Exclude the SNP's that are not qualified.
5. CSP verifies whether certificate of authorization of SNP is revoked and choose the service offered by SNP with the maximum value and informs TCE about signed SLA or PLA.
6. CSP checks whether certificate of SNP is revoked before its utilization. After the end of service, CSP sends feedbacks based on SLA and PLA about the service of SNP to TCE.

ANALYSIS AND RESULTS

The user has to construct the network and securely establish a connection between each node. For easy analysis, the user must give total number of node as input and also name each node.

Table 1. Analysis of Existing and Proposed system

	Existing %	Proposed %
CSP	55.60	90
SNP	65	88.70
CH	70	95



After this, the name or IP address of each node the user must make a simplex communication or duplex communication between each node. Thus network construction should be made.

Conclusion and future work

In this scheme, we have discussed and explored the rarely exposed sides of CC-WSN's alliance with r reliability and reputation calculation and management of CSP and SNPs respectively. The discussion and analysis of results proven to be highly efficient, secure and the performance evaluation of this scheme makes this feasible to integrate with An Accredit Reliability and Reputation Calculation and Management Scheme for Cloud and wireless Sensor Networks Alliance with respect to service provided by the CSP and SNP. As computed, this scheme achieved Accrediting of CSP's and SNP's to avoid any malicious attacks that replicate the data, calculating and managing reliability and reputation of CSP's and SNP's and assisting CSU in choosing CSP; assisting CSP to select appropriate SNP for alliance based on authorization of CSP and SNP, the attribute requirement of CSP and CSU, operational cost, reliability and reputation of CSP service. In addition, these three adversary models empowers security analysis showed that our proposed system is secure versus impersonation attacks on a trust and reputation management system, such ad good and bad mouthing, white-washing and collusion attacks, which may yield terrible results.

REFERENCES

Akyildiz F., W. Su, Y. Sankarasubramaniam, and E. Cayirci, 2002. "Wireless sensor networks: A survey, "Comput. Netw., *Int. J. Comput. Telecommun. Netw.*, Vol. 38, no. 4, pp. 393–422, Mar.

Buyya R., C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, 2009. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generat. Comput. Syst.*, vol. 25, no. 6, pp. 599–616, Jun.

Ganeriwal, S., L. K. Balzano, and M. B. Srivastava, 2008. "Reputation-based framework for high integrity sensor networks," ACM Trans. Sensor Netw., vol. 4, no. 3, May, Art. ID 15.

Govindan K. and P. Mohapatra, 2012. "Trust computations and trust dynamics in mobile adhoc networks: A survey," IEEE Commun. Surveys Tuts, Vol. 14, no. 2, pp. 279–298, Second Quarter.

Grzonkowski S. and P. Corcoran, 2011. "Sharing cloud services: User authentication for social enhancement of home networking," *IEEE Trans. Consum. Electron*., vol. 57, no. 3, pp. 1424–1432, Aug.

Li M. and Y. Liu, 2009. "Underground coal mine monitoring with wireless sensor networks," *ACM Trans. Sensor Netw*., vol. 5, no. 2, Mar. Art. ID 10.

Reece, S., A. Rogers, S. Roberts, and N. R. Jennings, "Rumours and reputation: Evaluating multi-dimensional trust within a decentralized reputation system," in Proc. 6.

Ruj, S., M. Stojmenovic, and A. Nayak, 2014. "Decentralized access control with anonymous authentication of data stored in clouds," IEEE Trans. *Parallel Distrib. Syst*., Vol. 25, no. 2, pp. 384–394, Feb.

Yuriyama M. and T. Kushida, 2010. Sensor-cloud infrastructure—Physical sensor management with virtualized sensors on cloud computing,‖ in Proc. 13th *Int*. *Conf. Netw.-Based Inf. Syst*., Sep. pp. 1–8.

Yuriyama M. and T. Kushida, 2010. Sensor-cloud infrastructure—Physical sensor management with virtualized sensors on cloud computing,‖ in Proc. 13th Int. Conf. Netw.-Based Inf. Syst., Sep. pp. 1–8.

Zhu, C., V. C. M. Leung, L. T. Yang, X. Hu, and L. Shu, 2013. Collaborative location-based sleep scheduling to integrate wireless sensor networks with mobile cloud computing,‖ in Proc. IEEE Globecom Workshops, Dec. pp. 452–457.

****