International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 05 Special Issue 01 | 2020

A Review on Authenticate Trusted Calculation Management system for Integration of Cloud-Computing and WSN

Girish Patil[1], Dr. Ajay Gadicha[2], Manjiri Karande[3]

[1] PG Student, Computer Science and Engineering, Padm. Dr. VBKCOE, Maharashtra, India
[2] Asst. Prof., Computer Science and Engineering, P. R. Pote COE and Management, Maharashtra, India
[3] Asst. Prof., Computer Science and Engineering, Padm. Dr. VBKCOE, Maharashtra, India

ABSTRACT

Recently from last few decades lots of work has been done in field of Cloud computing (CC) and Wireless sensor network (WSN). These two different fields play a major role to take attentions of researchers now a days when it comes to the integration of Cloud computing – Wireless sensor network both in the academia and the industry as it provides many opportunities for organizations by offering a range of computing services. That's why data gathering becomes easy with the help of integrated CC-WNS. But using cloud computing which as it is much popular in enterprises and individuals has some issues that has to be solved. In any case, authentication as well as trust and reputation calculation and management System (ATRCM) of cloud service providers (CSPs) and sensor network suppliers (SNPs) are two exceptionally critical and barely explored issues for this new paradigm. To overcome with this issue, here one idea for integration of authenticated trust and reputation calculation with CC-WSN has been given in this paper. This can be achieved by using TPA. A TPA is third party auditor which is trusted authority for two different parties. TPA performs verification on data which are stored on cloud or database. One party request TPA for their trust verification with other party and then TPA verify data by previous history matching other party and decides. Considering the authenticity of CSP and SNP, the attribute necessity of cloud service user (CSU) and CSP, the expense, trust, and reputation of the service of CSP and SNP, the system accomplishes the three functions: 1) avoid CSP and SNP from malicious impersonation attacks; 2) computing and managing trust and reputation with respect to the service of CSP and SNP; and 3) helping CSU choose desirable CSP and assisting CSP in selecting suitable SNP. Along with these function system security is provided.

Keyword: - TPA, Cloud, Wireless Sensor Network (WSN), Authenticate, Trusted, Reputation, Integration.

1. INTRODUCTION

Computing is being transformed to a model consisting of services that are commoditized and delivered in a manner similar to traditional utilities such as water, electricity, gas, and telephony. In such a model, users access services based on their requirements without regard to where the services are hosted or how they are delivered. Several computing paradigms have promised to deliver this utility computing vision and these include cluster computing, Grid computing, and more recently Cloud computing. The latter term denotes the infrastructure as a ``Cloud" from which businesses and users are able to access applications from any wherein the world on demand. Thus, the computing world is rapidly transforming towards developing software for millions to consume as a service, rather than to run on their individual computers [1]. Cloud computing (CC) is a model to enable convenient, on-demand network access for a shared pool of configurable computing resources (e.g., servers, networks, storage, applications, and services) that could be rapidly provisioned and released with minimal management effort or service provider interaction. Wireless sensor networks (WSNs) are networks consisting of spatially distributed autonomous sensors, which are capable of sensing the physical or environmental conditions.

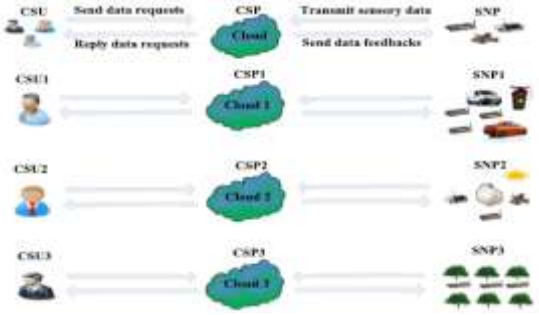

Fig 1. Integration of CC and WSN

1.1 Cloud Computing

With the rapid development of processing and storage technologies and the success of the Internet, computing resources have become cheaper, more powerful and more ubiquitously available than ever before. This technological trend has enabled the realization of a new computing model called cloud computing, in which resources (e.g., CPU and storage) are provided as general utilities that can be leased and released by users through the Internet in an on-demand fashion. In a cloud computing environment, the traditional role of service provider is divided into two: the infrastructure providers who manage cloud platforms and lease resources according to a usage-based pricing model, and service providers, who rent resources from one or many infrastructure providers to serve the end users. The emergence of cloud computing has made a tremendous impact on the Information Technology (IT) industry over the past few years, where large companies such as Google, Amazon and Microsoft strive to provide more powerful, reliable and cost-efficient cloud platforms, and business enterprises seek to reshape their business models to gain benefit from this new paradigm[2].

CLOUD computing (CC) is a model to enable convenient, on-demand network access for a shared pool of configurable computing resources (e.g., servers, networks, storage, applications, and services) that could be rapidly provisioned and released with minimal management effort or service provider interaction [3]. CC is featured by that users can elastically utilize the infrastructure (e.g., networks, servers, and storages), platforms (e.g., operating systems and middle ware services), and software (e.g., application programs) offered by cloud providers in an on-demand manner.

1.2 Wireless Sensor Networks (WSN)

A network called Wireless sensor networks (WSNs) are networks consisting of spatially distributed autonomous sensors, which are capable of sensing the physical or environmental conditions (e.g., temperature, sound, vibration, pressure, motion, etc.) [3]. WSNs are widely focused because of their great potential in areas of civilian, industry and military (e.g., forest fire detection, industrial process monitoring, traffic monitoring, battlefield surveillance, etc.), which could change the traditional way for people to interact with the physical world. For instance, regarding forest fire detection, since sensor nodes can be strategically, randomly, and densely deployed in a forest, the exact origin of a forest fire can be relayed to the end users before the forest fire turns uncontrollable without the vision of physical fire. A Wireless Sensor Network (WSN) is a self-organized wireless network composed of a large number of sensor nodes that interact with the physical world. Various low-power and cost-effective sensor platforms have been developed based upon recent advances in wireless communication and micro system technologies. The increasing study of WSNs aims to enable computers to better serve people by automatically monitoring and interacting with physical environments.

1.3 CC-WSN Integration

Powerful data storage and data processing abilities of CC as well as the ubiquitous data gathering capability of WSNs, CC-WSN integration captured much attention from both academic and industrial communities. This integration paradigm is driven by the potential application scenarios. [3] Specifically, sensor network providers (SNPs) provide the sensory data(e.g., traffic, video, weather, humidity, temperature) collected by the 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). Thus CSUs can have access to their required sensory data with just a simple client to access the cloud [3]. In this new paradigm, SNPs are the data sources for CSPs, and CSUs act as the data requesters for CSPs. The CC-WSN integration is as shown in figure 1.

2. RESEARCH MOTIVATION

However, during the CC-WSN integration, the following two very critical and barely explored issues should be taken into consideration. These two issues not only seriously impede the CSU from obtaining the desirable service they want from the authentic CSP, but also prevent the CSP from obtaining the satisfied service from the genuine SNP.

- Authentication of CSPs and SNPs
- Trust and Reputation Calculation and Management of CSPs and SNPs

3. LITERATURE REVIEW

3.1 Formal Modeling for Multi-Level Authentication in Sensor-Cloud Integration System

Recent developments in sensor networking require the need for integration of sensor networks with the cloud. This improves the processing power and battery life of the sensor nodes. Once the sensor data is routed to the cloud, possible measures need to be adopted to secure the sensor data. Thus, strict authentication checks have to be provided to facilitate authorized customers to utilize the services provided by the cloud in the form of

sensor data. In this paper, we present an authentication system by employing the multi-level authentication technique in securing the sensor data in cloud. This technique generates/authenticates the password in multiple levels to access cloud services. Thus, the proposed scheme helps in improving the authentication level by order of magnitude as compared to the existing technique. Thus, we expect, with this proposed technique the probability unauthorized accesses can be greatly reduced [4].

The expectation is to help in the analysis and provision of authenticated access to the data in the sensor-cloud integration system. We have described this authentication system by employing the multi- level authentication technique to secure the sensor data in cloud. This technique generates/authenticates the password at multiple levels to access cloud services. A strict authentication and authorization can be achieved through this technique. The proposed System is modelled using Petri net. Detailed analysis with respect to authentication scheme may be carried out. Our future work will be carried out in adding multi-dimensional password generation method to this system.

3.2 A Strong User Authentication Framework for Cloud Computing

Strong user authentication is the paramount requirement for cloud computing that restrict illegal access of cloud server. It requires a strong user authentication framework for cloud computing, where user legitimacy is strongly verified before enter into the cloud. The proposed framework provides identity management, mutual authentication, session key establishment between the users and the cloud server. A user can change his/her password, whenever demanded. Furthermore, security analysis realizes the feasibility of the proposed framework for cloud computing and achieves efficiency. This article proposes a strong user authentication framework for cloud computing with many security features, such as identity management, mutual authentication, session key agreement between the users and the cloud server, and user friendliness (i.e., password change phase). In addition, cloud computing being a combination of computing resources; resource constrains are given less priority to provide high security to the cloud. Hence, this article has not performed any performance comparison with some existing schemes. The proposed protocol can resist many popular attacks such as replay attack, man in the middle attack, and denial of service attack. Currently, study on some formal security proofing technique of is on process [5].

3.3 A Cloud Design for User-controlled Storage and Processing of Sensor Data

Cloud computing promises to elastically store and process such sensor data. As an additional benefit, storage and processing in the Cloud enables the efficient aggregation and analysis of information from different data sources. However, sensor data often contains privacy-relevant or otherwise sensitive information. For current Cloud platforms, the data owner loses control over her data once it enters the Cloud. This imposes adoption barriers due to legal or privacy concerns. Hence, a Cloud design is required that the data owner can trust to handle her sensitive data securely. In this paper, we analyze and define properties that a trusted Cloud design has to full fill. Based on this analysis, we present the security architecture of Sensor Cloud. Our proposed security architecture enforces end-to-end data access control by the data owner reaching from the sensor network to the Cloud storage and processing subsystems as well as strict isolation up to the service-level. Here results show that proposed security architecture is a promising extension of today's Cloud offers [6].

As considering outsourcing storage and processing of sensor data to the Cloud, multiple possibly unknown or untrusted stakeholders become involved.. The Trust Point has three things i) implements transport security mechanisms for communication with the Cloud, ii) applies object security mechanisms to outbound data items, and iii) performs key management for authorized services.

3.4 A Survey on Sensor-Cloud: Architecture, Applications, and Approaches

Wireless sensor network (WSN) applications have been used in several important areas because of its limitations of WSNs in terms of memory, energy, computation, communication, and scalability, efficient management of the large number of WSNs data in these areas is an important issue to deal with. There is a need for a powerful and scalable high-performance computing and massive storage infrastructure for real-time processing and storing of the WSN data as well as analysis (online and offline) of the processed information under context using inherently complex models to extract events of interest. In this scenario, cloud computing is becoming a promising technology to provide a flexible stack of massive computing, storage, and software services in a scalable and virtualized manner at low cost [7].

The Sensor-Cloud architecture enables the sensor data to be categorized, stored, and processed in such a way that it becomes cost-effective, timely available, and easily accessible. Most WSN systems which were included to several controlling/monitoring schemes were closed in nature, zero, or less interoperability, specific application oriented, and non extensible. However, integrating the existing sensors with cloud will enable an open, extensible, scalable, interoperable, and easy to use, reconstructible network of sensors for numerous applications. This article discussed the opportunities of implementing the technology to handle more complex situations of a real world through the service innovation capability of Sensor-Cloud infrastructure.

3.5 Trust Cloud: A Framework for Accountability and Trust in Cloud Computing

Key barrier to cloud computing is the lack of trust in clouds by potential customers. There is still little focus on detective controls related to cloud accountability and audit ability. The complexity resulting from the sheer amount of virtualization and data distribution carried out in current clouds has also revealed an urgent need for research in cloud accountability, as has the shift in focus of customer concerns from server health and utilization to the integrity and safety of end-users' data. This paper discusses key challenges in achieving a trusted cloud through the use of detective controls, and presents the Trust Cloud framework, which addresses accountability in cloud computing via technical and policy-based approaches.

To increasing accountability detective rather than preventive approaches are proposed. Detective approaches complement preventive approaches as they enable the investigation not only of external risks, but also risks from within the CSP. We have argued that the shift in end-users' concerns from system health and performance to the integrity and accountability of data stored in the Cloud requires a file-centric perspective, on top of the usual system-centric perspective for logging. By using Cloud Accountability Life Cycle and the abstraction layers of logs, it has identified the importance of both real-time and post-mortem approaches to address the nature of cloud computing at different levels of granularity. Our conceptual model potentially can be used to give cloud users a single point of view for accountability of the CSP. Currently researching and developing solutions for each layer, with one example being a logging mechanism for the system layer of cloud accountability [8].

4. EXISTING SYSTEM

In the Existing system integration of CC-WSN is carryout with the help of the following two aspects:
(A) Authentication,
(B) Trust and reputation.

(A) Authentication

In respect to authentication in CC-WSN integration, a cloud architecture which is extensible and secure for sensor information system is proposed in [09]. Here the proposed architecture composition and mechanism is describes first. After that it focus on security mechanism for authenticating legal users so that only legal users can access sensor data and information services inside the architecture, which is based on Kerberos protocol which issues a authority certificate for legal users. Lastly the architecture model has been proposed by prototype deployment and simulation.

Focusing also on securing sensor data for sensor-cloud integration systems by [10], a user authentication scheme is proposed by employing the multi-level authentication technique. It authenticates the password in multiple levels for users to access cloud services so as to improve authentication level by order of magnitude.

Concerning the authentication of the data generated by body sensor networks in [11], it presents, analyzes and validates a practical, lightweight robust data authentication scheme suitable for cloud-based health-monitoring. The main idea is to utilize a Merkle hash tree to amortise digital signature costs and use network coding to recover strategic nodes within the tree. Experimental traces of typical operating conditions show that over 99% of the medical data can be authenticated at very low overheads and cost.

To the best of our knowledge, current authentication schemes in CC-WSN integration only focus on authenticating users or data. Different from these schemes, our work concerns the authentication of CSPs and SNPs, which is an ignored but important issue in CC-WSN integration.

(B) Trust and reputation.

There are a number of research works with respect to trust or reputation of cloud (e.g., [12]–[14]). For example, focusing on the trustworthiness of the cloud resources in [15], a framework is proposed to evaluate the cloud resources trustworthiness, by utilizing an amor to constantly monitor and assess the cloud environment as well as checking the resources the armor protects. For efficient reconfiguration and allocation of cloud computing resources to meet various user requests, a trust model which collects and analyzes the reliability of cloud resources based on the historical information of servers is proposed in [16], so that the best available cloud resources to fulfil the user requests can be prepared in advance. To determine the credibility of trust feedbacks as well as managing trust feedbacks in cloud environments, [17] presents a framework named trust as service to improve current trust managements, by introducing an adaptive credibility model to distinguish the credible and malicious feedbacks. Discussing the cloud accountability issue in [18], it first uses detective controls to analyze the key issues to establish a trusted cloud and then gives a trust cloud framework consisted of five abstraction layers, where technical and policy-based approaches are applied to address accountability.

With respect to trust in the CC-WSN integration, the only related work is [19] focusing on how trust management could be effectively used to enhance the security of a cloud integrated WSN. Particularly, the

security breaches regarding data generation, data transmission and in-network processing in the WSN integrated with cloud are observed in [19] first. Then it shows some examples that trust can be employed to perform trust-aware data transmission and trust-aware data processing in the integrated WSN as well as trust-aware services in the cloud.

For the state of the art, there is no trust and reputation calculation and management system discussing CC-WSN integration. These two issues not only seriously obstacle the CSU from obtaining the desirable service they want from the authentic CSP, but also prevent the CSP from obtaining the satisfied service from the genuine SNP. In the authentication of CSPs and SNPs malicious attackers may impersonate authentic CSPs to communicate with CSUs, or fake to be authentic SNPs to communicate with CSPs. Then CSUs and CSPs cannot eventually achieve any service from the fake CSPs and SNPs respectively. In the meantime, the trust and reputation of the genuine CSPs and SNPs are also impaired by these fake CSP sand SNPs. [3] Without trust and reputation calculation and management of CSPs and SNPs, it is easy for CSU to choose a CSP with low trust and reputation. Then the service from CSP to CSU fails to be successfully delivered quite often. Moreover, CSP may easily select an untrustworthy SNP that delivers the service that the CSP requests with an unacceptable large latency.

5. CONCLUSION

Integration of CC-WSN along with the new concept of Third Party Auditor (TPA) overcomes two main obstacles

1) CSU will get the desirable services from their respective authentic CSP
2) Prevent the CSP from getting the satisfied services from their respective SNP ALONG with authentication, trust, reputation can be calculated.

Therefore during valid data transmission form WNS to CSP security (accessing, storage, transmission, and uploading) can be provided.

6. REFERENCES

[1]. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing andemerging IT platforms: Vision, hype, and reality for delivering computing as the 5thutility,"Future Generat. Comput. Syst., vol. 25, no. 6, pp. 599–616, Jun. 2009.
[2]. Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the art and researchchallenges," J. Internet Services Appl., vol. 1, no. 1, pp. 7–18, 2010.
[3]. Chunsheng Zhu, Student Member, IEEE, HasenNicanfar, Student Member, IEEE, Victor C. M. Leung, Fellow, IEEE, and Laurence T. Yang, Member, IEEE "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration", Ieee Transactions On Information Forensics And Security, Vol. 10, No. 1, January 2015
[4] H. A. Dinesha, R. Monica, and V. K. Agrawal, "Formal modeling for multi-level authentication in sensor-cloud integration system," Int. J. Appl. Inf. Syst., vol. 2, no. 3, pp. 1–6, May 2012.
[5] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, "A strong user authentication framework for cloud computing," in Proc. IEEE Asia-Pacific Services Comput. Conf., Dec. 2011, pp. 110–115.
[6] R. Hummen, M. Henze, D. Catrein, and K. Wehrle, "A cloud design for user-controlled storage and processing of sensor data," in Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci., Dec. 2012, pp. 232–240.
[7] A. Alamri, W. S. Ansari, M. M. Hassan, M. S. Hossain, A. Alelaiwi, and M. A. Hossain, "A survey on sensor-cloud: Architecture, applications, and approaches," Int. J. Distrib. Sensor Netw., vol. 2013, 2013, Art. ID 917923.
[8] R. K. L. Ko et al., "TrustCloud: A framework for accountability and trust in cloud computing," in Proc. IEEE World Congr. Services, Jul. 2011, pp. 584–588.
[9]. P. You and Z. Huang, "Towards an extensible and secure cloud architecture model for sensor information system," *Int. J. Distrib. Sensor Netw.*, vol. 2013, Jul. 2013, Art. ID 823418.
[10]. H. A. Dinesha, R. Monica, and V. K. Agrawal, "Formal modeling for multi-level authentication in sensor-cloud integration system," *Int. J. Appl. Inf. Syst.*, vol. 2, no. 3, pp. 1–6, May 2012.
[11]. S. T. Ali, V. Sivaraman, and D. Ostry, "Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring," *Future Generat. Comput. Syst.*, vol. 35, pp. 80–90, Jun. 2014.
[12]. K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Comput.*, vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.
[13]. A. Barsoum and A. Hasan, "Enabling dynamic data and indirect mutual trust for cloud computing storage systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 12, pp. 2375–2385, Dec. 2013.
[14]. X. Li and J. Du, "Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing," *IET Inf. Secur.*, vol. 7, no. 1, pp. 39–50, Mar. 2013.
[15]. M. Kuehnhausen, V. S. Frost, and G. J. Minden, "Framework for assessing the trustworthiness of cloud resources," in *Proc. IEEE Int. Multi-Discipl. Conf. Cognit. Methods Situation Awareness Decision Support*, Mar. 2012, pp. 142–145.
[16]. H. Kim, H. Lee, W. Kim, and Y. Kim, "A trust evaluation model for QoS guarantee in cloud systems," *Int. J. Grid Distrib. Comput.*, vol. 3, no. 1, pp. 1–9, 2010.
[17]. T. H. Noor and Q. Z. Sheng, "Trust as a service: A framework for trust management in cloud environments," in *Proc. 12th Int. Conf. Web Inf. Syst. Eng.*, 2011, pp. 314–321.
[18]. R. K. L. Ko *et al.*, "TrustCloud: A framework for accountability and trust in cloud computing," in *Proc. IEEE World Congr. Services*, Jul. 2011, pp. 584–588.
[19] O. Savas, G. Jin, and J. Deng, "Trust management in cloud-integrated wireless sensor networks," in *Proc. Int. Conf. Collaboration Technol. Syst.*, May 2013, pp. 334–341.