Survey on integration of cloud computing and WSN to identify best Cloud service provider

Ms.Vedambika M
M.Tech Scholar, Dept. of Computer Science and Engineering,
New Horizon College of Engineering,
Bangalore, India
E-mail: veda299@gmail.com

Ms. Soja Rani S
Assistant professor,
Dept. of Computer Science and Engineering,
New Horizon college of Engineering
Bangalore, India
***E-mail:* soja.naveen@gmail.com**

Abstract-Wireless Sensor Networks are used to sense the environment conditions and collect the information. The collected information is stored in the cloud in which the user can access the required information. The integration of both cloud service provider and sensor network provider will provide the effective service to the cloud service user. This paper is a general survey of all the sensor network provider and cloud service provider integration. The majority of the survey is mainly focused on the authenticated trust and reputation calculation for sensor network provider and cloud service provider.

Keywords– cloud computing,* sensor network, *authentication, reputation, trusts andintegration.

I. INTRODUCTION

A cloud is a huge group of interconnected computer system which extends beyond single company or enterprise. The cloud will serve the applications and data which are accessed via the Internet by group of users of multiple enterprises and platforms. A cloud computing system consists of interconnected and virtualized computers which dynamically provisioned as one or more unified computing resource(s) over negotiation of service-level agreements (SLAs) between providers and consumers. Resources have to be energetically configured and combined via virtualization and consumer's requirements possibly fluctuate over time and changes need to be accommodated.

Wireless Sensor Networks (WSN), naturally distributed in nature, are distributed across the globe. A WSN consists sensor nodes which monitor physical, environmental, or human conditions such as temperature, sound, vibration, pressure, motion, heart rate, and blood pressure. WSN nodes emit a huge amount of dense, contextual data about an environment. The skill of a sensor network are not only observing and forwarding sensor readings. These sensor networks senses the raw data from the wider application domain. The wireless sensor networks also provide many different services like traffic control, awareness in military situation, monitoring the home automation system, healthcare, and weather forecasting.

Sensor networks help to gather information and stores the data for a long period of time. This storing of sensor data is achieved by using storages and these storage data is computed. Precisely, the sensor networks enables to store the data, process the stored data, and access the collected sensor data excellently via Cloud-based services.

A huge amount of data is stored in the clouds these are sensitive data, for example military records, social networks and medical records. So the security and privacy are the two main issues which has to mandatory handle in cloud computing. The user has to authenticate before the initialization of any transaction and also it must be ensure that the data is not tampered or leaked to any malicious node or user while outsourcing the data. User privacy provides that the cloud and other users should not be in a position to identity of the intended user.

The cloud helps to store the user accountable data which it's outsourced and like-wise cloud itself maintain accountable data for which service it provides. Validity for the user stored data is also verified. Except these technical solutions to ensure security and privacy, there should be also taking care of non-technical solution. This will be providing by the law enforcement...secure data storage is achieved through the encryption of the stored data. The network has to be designed in the sense that when the data is modified the network has to be process properly. This are achieved through by making use of efficient secure storage techniques.

Evaluation of the reputation is done by users and resource owners. Earlier researchers have invented much reputation for e-commerce, multi-agent, or P2P systems. To funding trusted cloud services, the best way is to design trust-overlay network to provide relationships between data-center modules.

While there is no universally accepted definition of trust in cloud computing, it is important to clarify its components and meaning. In dictionaries, trust is generally related to “levels of confidence in something or someone”. Hence we can view trust in the cloud as the customers’ level of confidence in using the cloud, and try to increase this by mitigating technical and psychological barriers to using cloud services.

II RELATED WORK

Qi Zhang et.al, 2010Cloud computing: state-of-the-art and research challenges [1]. Cloud computing has made rapid changes to information technology, and ultimately turning the long-held promise of utility computing into a reality. The key challenges in this domain, including automatic resource provisioning, power management and security management. Therefore, we believe there is still tremendous opportunity for researchers to make groundbreaking contributions in this field, and bring significant impact to their development in the industry.
In this paper they have surveyed the state-of-the-art of cloud computing, covering its essential concepts, architectural designs, prominent characteristics, key technologies as well as research directions.

KwangMong Sim,2012 Agent-Based Cloud Computing [2]. The significance of this work is by presenting applying the operator to putting together the merchandise devices and check for overseeing cloud assets, this work they need done advances the state in 2 ways in which. From the cloud computing perspective, this work adds to the sector of cloud plus administration by formulating a number of ways in which to cope with encourages the cloud administration revelation, administration group action, and administration structure. From the multi operator systems perspective, this work exhibits the utilization of 1) agreeable important thinking ways to mechanizing cloud administration organization, 2) unpredictable and synchronic arrangements to cloud business, and 3) programming specialists to putting together a cloud internet crawler.

Giancarlo Fortino et.al, 2012BodyCloud: Integration of Cloud Computing and Body Sensor Networks [3]. Body Cloud may be a Cloud Computing framework engineering for the administration and checking of body sensing element data streams. The framework offers a stage to fabricate and send applications taking into consideration body sensing element systems. Framework properties incorporate skillfulness and adaptableness of assets, capability to supervise part or device heterogeneousness and therefore the element organization of consumer and cluster applications. Current endeavors square measure committed to the usage and testing of the framework. Future work can incorporate the advancement of experiments which may exhibit the scope of utilizations that square measure authorized by the framework.

Ren´eHummen et.al, 2012: A Cloud Design for User-controlled Storage and Processing of Sensor Data [4]. While outsourcing capability and making ready of sensing element data to the Cloud, various probably obscure or untrusted partners get to be enclosed. During this paper, we tend to distinguish the actual dangers that emerge from this questionable contribution. Our projected Sensor Cloud security engineering counters these dangers by allowing businessman to remain up to speed over her information even in a very Cloud scenario. To the present finish, we tend to gift a Trust purpose as another legitimate substance that's set at the fringe of the sensing element system and goes regarding as a scaffold between the protection house of the sensing element system and therefore the Cloud. The Trust purpose i) executes transport security elements for correspondence with the Cloud, ii) applies object security instruments to outward-bound data things, and iii) performs key administration for approved administrations. To alleviate spillage of touchy knowledge from the run-time connections of administrations, we tend to additionally propose the utilization of segregation instruments as way as doable up to the administration level. Our assessment demonstrates that our projected sensing element Cloud security style incorporates an adequate execution for the expected scenario which the enclosed reposition and memory overheads will be taken care of adequately.

Chunsheng Zhu et.al, 20

15: Collaborative Location-Based Sleep Scheduling for Wireless Sensor Networks Integrated with Mobile Cloud Computing [5]. In this paper, we've got projected 2 CLSS plans (i.e., CLSS1 and CLSS2) for WSNs incorporated with MCC. CLSS plans embody each the WSN and therefore the cloud and then dynamically modification the aware or snoozing standing of the sensor node within the incorporated WSN, in sight of the areas of moveable shoppers. CLSS1 concentrates on frugal the foremost vitality utilization of the incorporated WSN and CLSS2 any pays thought on the flexibility and wholeheartedness of the coordinated WSN. For the reconciliation of MCC and WSNs, each theoretical and recreation results square measure appeared and that they exhibit that CLSS1 what's additional, CLSS2 may drag out the time period of the coordinated WSN whereas till now fulfilling the data solicitations of versatile shoppers.

Victor C. M. Leung et.al, 2013: Providing Desirable Data to Users when Integrating Wireless Sensor Networks with Mobile Cloud [6]. The coordination of remote sensing element systems (WSNs) and versatile distributed computing (MCC) is loosely engaged. In this paper, concentrating on comprehending the association non-mindfulness issue that we tend to see between the moveable consumer and therefore the WSNs, We provide a novel structure to administer seductive data to moveable shoppers once incorporating WSNs and MCC. The projected system makes note of the data proposal, data forecast too data activity checking so as to accomplish the versatile consumer data inclinations highlight knowledge and in addition WSNs potential standing data. With these data regarding moveable consumer needed data and WSNs data, we tend to direct the improved organization of WSNs and check the standing of WSNs. The adequacy of the projected structure is sealed by broad assessments.

SlawomirGrzonkowski et.al. 2011: Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking [7]. A confirmation system for home systems is presented. A configuration for the important confirmation conventions utilizing zero-information verification (ZKP) procedures is given, allowing the employment of a simple client/secret key validation. Since the client/secret key ne'er leaves the confirming contraption this keeps associate degree abnormal state of security and therefore the danger of "breaking" the administration is proscribed to the "trusted" home atmosphere. Notwithstanding further knowledge transfer capability and machine necessities it's incontestable that such a technique is accomplishable with satisfactory verification postpones and utilizing a scope of today's metal cellular phone gadgets. The projected framework offers consumer driven validation as any contraption with a Web program will produce a login screen and execute the client/watchword hashing to recover the specified key private/open key pair.

Conclusion

Based on the survey from the above paper the cloud service provider and the sensor network provider are integrated. The best service provider is found by the client using the rank voting method. This is calculated by certain criteria like the cost of the service, platform, SLA, capacity, certification, OS etc. the best service provider is also calculated by the user feedback that is rating the provider with highest rating will be the best provider. The sensor collects the data and that data is stored in the service provider which can be accessed by the user. The authentication, reputation, and trust calculation is most important . The user authentication is possible by giving the username and password. Reputation is based on the user rating to the service provider. By this we can achive 1) authenticating CSP and SNP to avoid malicious impersonation attacks; 2) calculating and managing trust and reputation regarding the service of CSP and SNP; 3) helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP.

REFERENCES

[1] Q. Zhang, L. Cheng, and R. Boutaba, “Cloud computing: State-of-the art and research challenges,” *J. Internet Services Appl.*, vol. 1, no. 1, pp. 7–18, 2010.

[2] K. M. Sim, “Agent-based cloud computing,” *IEEE Trans. Services Comput.*, vol. 5, no. 4, pp. 564–577, Fourth Quarter 2012.

[3] G. Fortino, M. Pathan, and G. Di Fatta, “BodyCloud: Integration of cloud computing and body sensor networks,” in *Proc. IEEE 4th Int.Conf. Cloud Comput. Technol. Sci.*, Dec. 2012, pp. 851–856.

[4] R. Hummen, M. Henze, D. Catrein, and K. Wehrle, “A cloud design for user-controlled storage and processing of sensor data,” in *Proc. IEEE4th Int. Conf. Cloud Comput. Technol. Sci.*, Dec. 2012, pp. 232–240.

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

[6] C. Zhu, V. C. M. Leung, H. Wang, W. Chen, and X. Liu, “Providing desirable data to users when integrating wireless sensor networks with
Mobile cloud,” in *Proc. IEEE 5th Int. Conf. Cloud Comput. Technol. Sci.*, Dec. 2013, pp. 607–614.

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

[8] 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.

[9] S.-H. Shin, D.-H.Kim, and K.-Y. Yoo, “A lightweight multi-user authentication scheme based on cellular automata in cloud environment,”
InProc. *IEEE 1st Int. Conf. Cloud Netw.*, Nov. 2012, pp. 176–178.

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

[11] 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.

[12] 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.

[13] 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.

[14] R. K. L. Koet *al.*, “TrustCloud: A framework for accountability and trust in cloud computing,” in *Proc. IEEE World Congr. Services*, Jul. 2011, pp. 584–588.