Third Party Application for Providing Authentication trust and Reputation Calculation Management in Cloud Computing and Wireless Sensor Network Integration

Mr. M. V. Shastri[1], Ms. Farisa Fatema[2], Ms. Tejaswini Pathak[3], Ms. Samruddhi Pol[4], Ms. Shweta Rajput[5]

[1, 2, 3, 4, 5] *Department of Computer Science & Engineering, Dr. V. B. kolte College of Engineering, Malkapur , India*

ABSTRACT

The Powerful data storage that cloud provide us as well as the tremendous data gathering capability of wireless sensor network , and the combination of the both the cloud computing and wireless sensor network grab the attention from the every medium . But the trust and reputation calculation and management system are the very critical issue in the today's era.

To overcome this problem, this paper proposes a solution to this problem that i.e. it provide authentication to the trust and reputation calculation management t system for the cloud computing, and the wireless sensor network integration. By considering the authentication of each and every participant of the system ,the main requirement of the every participant .Our Proposed System Provide the following key characteristics 1)Authentication to the cloud service provider and sensor network provider to avoid attacks 2)Calculating and managing trust and reputation to regarding to the service of cloud service provider and sensor network provider 3)It help the Cloud service user to choose it's cloud service provider and sensor network provider .

Index items/ keywords – Cloud, Sensor network, Integration, Authentication, Reputation, Calculation, trust.

1. INTRODUCTION

Trust management is the important issue for the growth of the each and every thing. The highly dynamic, distributed and Non transparent issue of the cloud service introduces several challenges in term of data privacy, security and the availability .Protecting Consumers Privacy is not the simple task because it contain the sensitive data involved in the interaction between the Consumers , the trust and reputation management service . This is difficult problem to protect the cloud service from their malicious users. There is no guarantee of the availability of the trust management this is another challenge because of the dynamic nature of the cloud service . In this we describe the design and implementation of the cloud weapon, A reputation contain trust management design that provides the set of functionalities i.e. it provide the Trust as a Service .

2. CLOUD COMPUTING

Cloud Computing is a model to get the convenient on demand network access for the shared pool of configurable computing resources .We can say it is a on –demand availability of resources ,mainly data storage and power of computing , without the direct management by the user . This term is generally used to describe the data centers available to many user over the internet .The term cloud may be limited to single organization (i.e. enterprise cloud) and may be also available to many organizations (i.e. public cloud).

3. WSN

WSN stands for the wireless sensor network. This term refers to a group of scatter and dedicated sensors for the recording and monitoring the physical condition of the surrounding and recognizing the collected data at a central location. These network measure environmental conditions like temperature, sound, pollution levels, humidity, wind and so on.

4. CC-WSN INTEGRATION

This integration prototype is given by the potential application scenarios which are shown in the figure. The working of sensor network providers (SNPs) is to provide the sensory data (i.e. Traffic, Temperature, weather which is collected by the wireless sensor network which are deployed and the data is that provided to the cloud service provider CSPs. Cloud service provider make use the powerful cloud to store and process the data which is provided by the sensor and after getting the data on demand it provide it to the cloud service in that way the cloud service users. Thus the Cloud service user can get access to their required data which is provided by sensor in the simple way the client has to get access to the cloud. In this way a new prototype the sensor network provider are the sources of the data for the cloud service provider and the cloud service user. The cloud service provider and cloud service user behave as the data requesters for the cloud service provider.

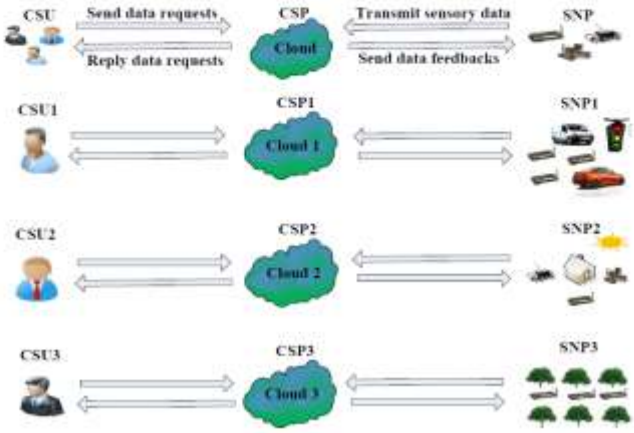

Fig. 1. Example of application scenarios of CC-WSN integration.

5. EXISTING SYSTEM

In the existing system the data has to travel a longer path from cloud service provider to the cloud service user. we can say the data from the sensor network provider to the cloud service provider in between that the data will get intentionally or by some technical reason it will be changed and modify and destroy by the attacker. It creates the problems for the user.

By Considering an example regarding the forest fire detection in that case sensors are displayed in the forest fire turn out of the control in that case we use our system to get the proper origin of the fire .

5.1 Disadvantages

1. Security provided in terms of the authentication is less.
2. We can’t trust the cloud in order to get the trusted information
3. The data has to travel the longer path due to this problem the delay is get occur in accessing the information

6. PROPOSED SYSTEM

According to the research of the different researchers at Barkley, the trust and security is at the top of 10 obstacle the user faces during accessing the data or for the adoption of cloud computing . Apart from this, the Service level arguments consumers’ feedback is the good source to assess the overall trustworthiness of the cloud. Most of the researchers have been identified the importance of trust management and suggest solutions to determine and manage trust based on the feedback gathered from researchers who take the part in the meeting.

By considering the following points we proposed the TPA (Third Party Application) for providing the authentication, trust, reputation management system (ATRCM) for the cloud computing and wireless sensor network integration. Points are as follows:

1. The Authentication to the Cloud service Provider and Sensor network Provider.
2. The main requirement of the cloud service user and cloud service provider.
3. The cost, trust and reputation these service of the cloud service provider.

6.1 Advantages of Proposed System

1. In our TPA (Third Party Application) there are different security policies or the authentication policies of the different domains
2. Our TPA (Third Party Application) considers the transaction context, the historical data of entity influences and the measurement of trust value dynamically .
3. Our TPA (third party application) overcomes all the drawbacks of the existing system.

7. FLOW OF THE SYSTEM

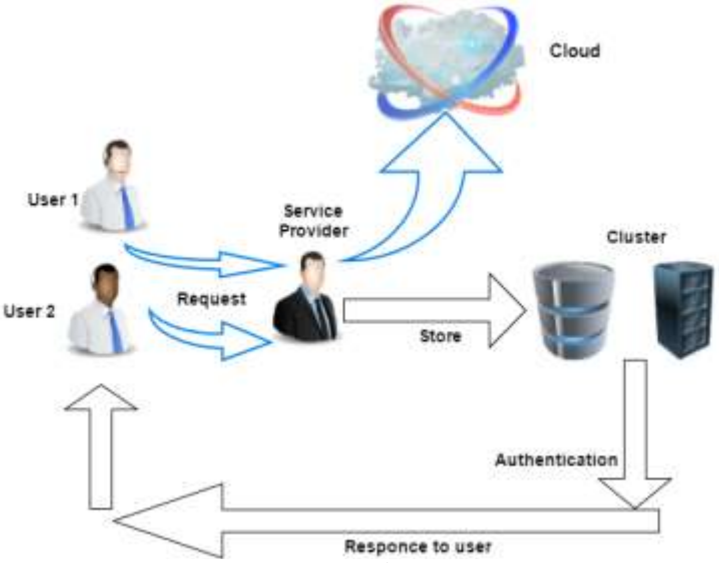

Fig 2 : Flow of System

In the above figure (i.e. Fig 2) two users are there who want the data from the cloud . In our proposed system one cluster is over there where historic data will get stored . whenever user wants something from the cloud it will send request to the cloud service provider .the cloud service user choose from which sensor network provider he wants to access the data . After that the cloud service user check the data (Sensory Data) present in the cloud and compare it with the historic data present in the cluster, after comparing both of them then it will send the trustworthy data to the user .

8. CONCLUSION

In this project we advancing explored the authentication as well as trust and reputation calculation management of cloud service providers and sensor network provider s, which are two very crucial and barely explored issues with respect to Cloud Computing and wireless sensor network integration . Further we proposed a important Authenticated trust and reputation calculation management system for CC-WSN (Cloud Computing – Wireless Sensor Network) integration.

Discussion the analysis about the authentication of cloud service provider and sensor network provider have been presented by following with the detail design about the proposed authentication trust and reputation calculation management system all these explain function of the proposed authentication trust and reputation management system achieves the three function for cloud computing – Wireless sensor network integration the functions are as follows :-

1) It will provide authentication to the cloud service provider and sensor network provider to avoid harmful attack
2) Calculating and managing trust and reputation regarding to the service of cloud service provider and sensor network provider
3) The system will also help the cloud service user to choose the its desirable cloud service provider and also assist the cloud service provider in order to select appropriate sensor network provider

In the addition, our TPA (Third Party Application) security analysis powered by three models. These models shows that our proposed system secured vs main attacks on a trust and reputation management system such as good mouthing and white washing attack which are the important attacks in our case .

9. REFERENCES–

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

[2] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “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. 2009.

[3] J. Baliga, R. W. A. Ayre, K. Hinton, and R. S. Tucker, “Green cloud computing: Balancing energy in processing, storage, and transport,” Proc. IEEE, vol. 99, no. 1, pp. 149–167, Jan. 2011.

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

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

[6] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wirelesssensor networks: A survey,” Comput. Netw., Int. J. Comput. Telecommun.Network ., vol. 38, no. 4, pp. 393–422, Mar. 2002.

[7] C. Zhu, L. Shu, T. Hara, L. Wang, S. Nishio, and L. T. Yang,“A survey on communication and data management issues in mobilesensor networks,” Wireless Commun. Mobile Comput., vol. 14, no. 1,pp. 19–36, Jan. 2014.

[8] M. Li and Y. Liu, “Underground coal mine monitoring with wirelesssensor networks,” ACM Trans. Sensor Netw., vol. 5, no. 2, Mar. 2009,Art. ID 10.

[9] M. Yuriyama and T. Kushida, “Sensor-cloud infrastructure—Physicalsensor management with virtualized sensors on cloud computing,” in Proc. 13th Int. Conf. Netw.-Based Inf. Syst., Sep. 2010, pp. 1–8.

[10] 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.

[11] Y. Takabe, K. Matsumoto, M. Yamagiwa, and M. Uehara, “Proposed sensor network for living environments using cloud computing,” in Proc.15th Int. Conf. Netw.-Based Inf. Syst., Sep. 2012, pp. 838–843.

[12] 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.

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

[14] C. Zhu, V. C. M. Leung, H. Wang, W. Chen, and X. Liu, “Providingdesirable data to users when integrating wireless sensor networks withmobile cloud,” in Proc. IEEE 5th Int. Conf. Cloud Comput. Technol.Sci., Dec. 2013, pp. 607–614.M. S. Hossain, A. Alelaiwi,

[15] 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.

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

[17] M.-H. Guo, H.-T. Liaw, L.-L. Hsiao, C.-Y. Huang, and C.-T. Yen,“Authentication using graphical password in cloud,” in Proc. 15th Int.Symp. Wireless Pers. Multimedia Commun., Sep. 2012, pp. 177–181.

[18] H. A. Dinesha and V. K. Agrawal, “Multi-dimensional password generationtechnique for accessing cloud services,” Int. J. Cloud Comput.,Services Archit., vol. 2, no. 3, pp. 31–39, Jun. 2012.

[19] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, “A stronguser authentication framework for cloud computing,” in Proc. IEEEAsia-Pacific Services Comput. Conf., Dec. 2011, pp. 110–115.

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

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

[22] J. Yang et al., “A fingerprint recognition scheme based on assemblinginvariant moments for cloud computing communications,” IEEE Syst. J.,vol. 5, no. 4, pp. 574–583, Dec. 2011.

[23] P. You and Z. Huang, “Towards an extensible and secure cloud architecturemodel for sensor information system,” Int. J. Distrib. Sensor Netw.,vol. 2013, Jul. 2013, Art. ID 823418.

[24] H. A. Dinesha, R. Monica, and V. K. Agrawal, “Formal modeling formulti-level authentication in sensor-cloud integration system,” Int. J.Appl. Inf. Syst., vol. 2, no. 3, pp. 1–6, May 2012.