European Journal of Molecular & Clinical Medicine

ISSN 2515-8260 Volume 07, Issue 11, 2020

A Software Defined Network Based Security Assessment Framework For Cloud Iot

[1] K. Vijay Kumar [2] Dr. T. Vijaya Saradhi

[1]M.Tech Scholar, Department of Computer Science and Engineering, Sreenidhi institute of science and technology.

[2]Professor of Computer Science and Engineering, Sreenidhi institute of science and technology.

Abstract

Cloud and Internet of Things incorporation (IoT), referred to as Cloud IoT, has been deemed an enabler for Lots of distinct implementations. Nevertheless the suspicion of the security problem is one of the key issues that some organizations are hesitant to implement such technologies, while some simply dismiss the technologies. security problem when incorporating Cloud IoT into their business. Therefore, given the numerous choices of cloud-resource providers and IoT devices, how to evaluate their security level becomes an important issue to promote the adoption of Cloud IoT as well as reduce the business security risks. In order to solve this issue, we are designing an end-to-end security assessment system based on Software Defined Network (SDN) to determine the security level for the provided Cloud IoT offering, considering the value of business data in Cloud IoT. Specially, in order to simplify the network controls and focus on the analysis about the data flow through Cloud IoT, we develop a three-layer framework by integrating SDN and Cloud IoT, which consists of 23 different indicators to describe its security features. Then, industry and academic interviews are conducted to recognize the value of these features for overall protection. In addition, our system can efficiently determine the level of protection that can assist customers in their Cloud IoT collection, provided the related evidence from the Cloud IoT offering, Google Brillo and Microsoft Azure IoT Suite.

1. INTRODUCTION

The Internet of Things (IoT) has recently emerged as a novel networking paradigm to connect a large amount of smart objects for data sharing and exchanging, so that we can measure, communicate and interact with the real physical world. On the other hand, cloud computing has been accepted as a cost-effective approach for providing high performance computing and virtually unlimited storage resource. Therefore, the integration of these two complementary technologies, the sensor-capability from IoT and the computing-capability from Cloud, has been accepted as a novel IT paradigm, named Cloud IoT, for many different applications, including smart grid, smart cities, healthcare, video surveillance environmental monitoring etc. Actually, the Cloud IoT is playing an important role for the current IT system, especially for the critical infrastructure.

2. RELATED WORK

Internet of Things (IoT): A vision, architectural elements, and future directions [1]

Ubiquitous sensing enabled by Wireless Sensor Network (WSN) technologies cuts across many areas of modern day living. This offers the ability to measure, infer and understand environmental indicators, from delicate ecologies and natural resources to urban environments. The proliferation of these devices in a communicating–actuating network creates the Internet of Things (IoT), wherein sensors and actuators blend seamlessly with the environment around us, and the information is shared across platforms in order to develop a common operating picture (COP). Fueled by the recent adaptation of a variety of enabling wireless technologies such as RFID tags and embedded sensor and actuator nodes, the IoT has stepped out of its infancy and is the next revolutionary technology in transforming the Internet into a fully integrated Future Internet. As we move from www (static pages web) to web2 (social networking web) to web3 (ubiquitous computing web), the need for data-on-demand using sophisticated intuitive queries increases significantly. This paper presents a Cloud centric vision for worldwide implementation of Internet of Things.

Body Cloud: A SaaS approach for community Body Sensor Networks [2]

Body Sensor Networks (BSNs) have been recently introduced for the remote monitoring of human activities in a broad range of application domains, such as health care, emergency management, fitness and behavior surveillance. BSNs can be deployed in a community of people and can generate large amounts of contextual data that require a scalable approach for storage, processing and analysis. Cloud computing can provide a flexible storage and processing infrastructure to perform both online and offline analysis of data streams generated in BSNs. This paper proposes Body Cloud, a SaaS approach for community BSNs that supports the development and deployment of Cloud-assisted BSN applications. Body Cloud is a multi-tier application-level architecture that integrates a Cloud computing platform and BSN data streams middleware. Body Cloud provides programming abstractions that allow the rapid development of community BSN applications. This work describes the general architecture of the proposed approach and presents a case study for the real-time monitoring and analysis of cardiac data streams of many individuals.

3. FRAMEWORK

Due to the on-time bypassing data transmission scheme, S-DTA can provide efficient and secure data transmission to various IoT devices in cloud networks.

ISSN 2515-8260 Volume 07, Issue 11, 2020

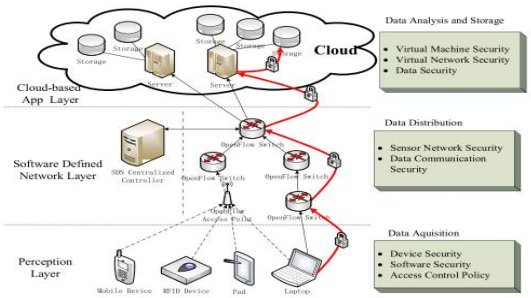

Fig.1: High-level data flow diagram of SDN-based Cloud IoT.

4. EXPERIMENTAL RESULTS

IoT (Internet of Things) are small devices such as smart phones, RFID, temperature sensing sensors or power grid sensors etc. This small devices sense data and then send to cloud servers for storage and processing. Cloud IoT are getting famous in various fields such as patient health monitoring (sensors will sense human body temperature, heart rate and send to hospital for monitoring), road side traffic monitoring and many more. This combination of IoT and cloud is lack of security and in this paper author has figured out 23 different security issues and then conduct a meeting with various professionals to give rating for each security features and using this rating dataset author is calculating rank to find which security features professionals are giving more importance.

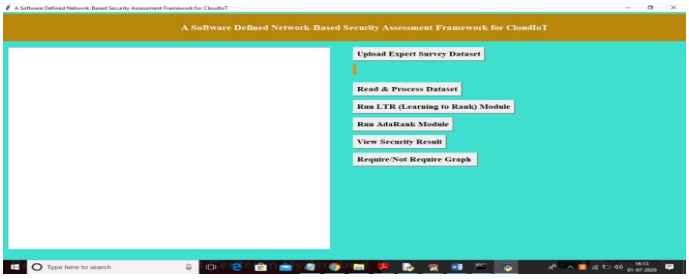

Fig.2: Home page

Fig.3 LTR Ranking

Fig.3 In above screen we can see LTR ranking for each feature and now click on 'Run Ada Rank Module' to predict which security is require (experts give more preference) and which security features not require (experts give less preference) by checking Ada Rank weight.

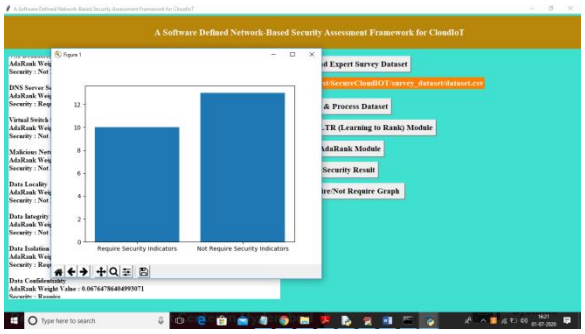

Fig.4 Ada Rank Weight

Fig.4: In above screen we can see each feature name and below it we can see Ada Rank weight value and then that security require or not require. In selected text we can see 'Antivirus and Antimalware' feature require and scroll down above text area to see result for each feature.

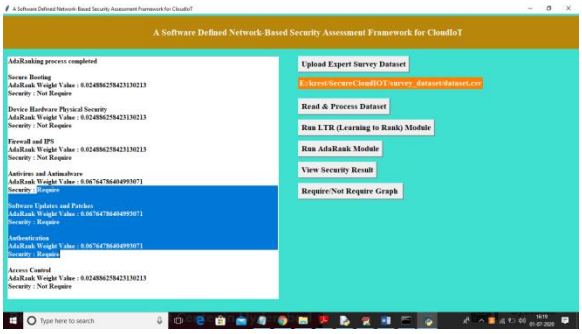

Fig.5 Indicator

Fig.5 In above graph x-axis represents features type as require or not require and y-axis represents count. From above graph we can conclude that out of 23 security features experts want or require 10 features and not require 13 features. Each security feature is called as indicator.

CONCLUSION

The integration of cloud computing and Internet of things (IoT) motivate the emergence of the Cloud IoT. Since the security has become one important issue for its adoption, how to evaluate the security level of the offered solution is valuable and necessary for consumers. In this paper, based on the analysis about the data flow over the Cloud IoT, we propose a SDN-based three-layer indication framework consisting of 23 indicators. To evaluate the importance of these indicators, we construct the online survey research

to invite experts from researchers and practitioners to rate the indicators and then three different methodologies to generate the aggregate rating are used to gain the weights. Given the weights for different indicators, taking the two real-world Cloud IoT solutions as an example, we identify the evidences for the related security mechanisms so that we can figure out how the solutions offer the security guarantee for customers. Therefore, we can offer the consumer the end-to-end approach to compare the security level of different solutions as well as to identify the weakness for the solution providers.

REFERENCES

[1] A. Prati, R. Vezzani, M. Fornaciari, and R. Cucchiara, "Intelligent Video Surveillance as a Service," Intelligent Multimedia Surveillance: Current Trends and Research, vol. 9783642415, no. November 2013, pp. 1–16, 2013.

[2] M. Armbrust, A. Fox, R. Griffith, A. Joseph, and RH, "Above the clouds: A Berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. UCB, pp. 07–013, 2009.

[3] 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 Generation Computer Systems, vol. 25, no. June 2009, p. 17, 2009.

[4] A. Botta, W. De Donato, V. Persico, and A. Pescape, "Integration of ´ Cloud computing and Internet of Things: A survey," Future Generation Computer Systems, vol. 56, pp. 684–700, 2016.

[5] M. D´ıaz, C. Mart´ın, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," Journal of Network and Computer Applications, pp. 1–19, 2015.

[6] J. Zhou, T. Leppanen, E. Harjula, M. Ylianttila, T. Ojala, C. Yu, and H. Jin, "CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing," Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2013, pp. 651–657, 2013.

[7] M. Yun and B. Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," in 2010 International Conference on Advances in Energy Engineering, ICAEE 2010, 2010, pp. 69–72.

[8] I. PodnarZarko, A. Antonic, and K. Pripuzic, "Publish/subscribe mid- ˇ dleware for energy-efficient mobile crowdsensing," Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication - UbiComp '13 Adjunct, pp. 1099–1110, 2013.

[9] A. Forkan, I. Khalil, and Z. Tari, "CoCaMAAL: A cloud-oriented context-aware middleware in ambient assisted living," Future Generation Computer Systems, vol. 35, pp. 114–127, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.future.2013.07.009

ISSN 2515-8260 Volume 07, Issue 11, 2020

[10] G. Fortino, D. Parisi, V. Pirrone, and G. Di Fatta, "BodyCloud: A SaaS approach for community Body Sensor Networks," Future Generation Computer Systems, vol. 35, pp. 62–79, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.future.2013.12.015