Fig. 30 shows the processing time for the revocation check with the number of users around 10 up to 1000 users. We analyze for 1000 revoked users there are only 2 second processing time for revocation check.

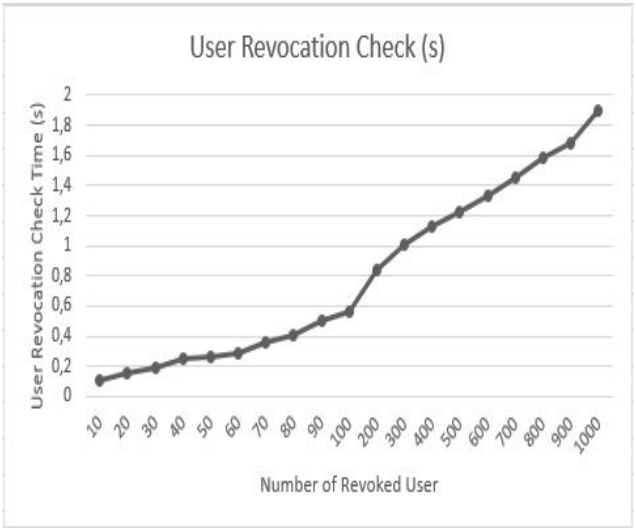

Fig. 30. Processing time for revocation check with 1000 user revoked

IV. CONCLUSIONS

We added a retraction on the method of CP-ABE to strengthen security for users who perform illegal access and protect the security of the system from the user is not responsible. Our revoke scheme do not affect the performance of the system from the data center environment health monitoring. The revocation list can only be accessed by the trust third party that is trusted by the manager and the user to perform monitoring and validation. Our experimental results showed the system requires less than 170 ms for the user with access right to encrypt the data for one month and requires less than160 ms to decrypt the data with 190 ms for transmission time. Compared with the user in revocation list with the same encryption time but requires the longer time for decrypt the data. to encrypt the data for one month user in revocation list requires less than 180 ms, for decrypt the data, user in revocation list requires less than 150 ms with 170 ms for transmission time. In embedded system our performance system only need less than 280 ms for transmission time for 1 Day, 285 ms for 1 week and also less than 290 ms for 1 month. Our experimental also showed time for the revocation check with amount 1000 users. The system requires less than 2 s for checking 1000 users. Our system with trust third party can control all of user in the data center from the illegal access, only third trust party can include the user to the revocation list and remove the user in the revocation list.

Our future work is including the digital time stamp signature to the messages sent by the manager to perform monitoring for the active user and add validity of the data from the data center and ensure there are no changes during the process of transmission data.

REFERENCES

[1] A.Sudarsono, M.U.H. Al Rasyid, An Anonymous Authentication System in Wireless Networks Using Verifier-Local Revocation Group Signature Scheme. International Seminar on Intelligent Technology and Its Application Technology, pp. 49-54, 2016.

[2] M.U.H. Al Rasyid, Bih-Hwang Lee, A.Sudarsono, and Taufiqurrahman, Implementation of Body Temperature and Pulseoximeter Sensors for Wireless Body Area Network. Sensors and Materials, International Journal on Sensor Technology. 27(8), pp. 727-732, 2015.

[3] S.Huda, A.Sudarsono, and T.Harsono, Secure Communication and Information Exchange using Authenticated Ciphertext Policy Attribute-Based Encryption in Mobile Ad-hoc Network. EMITTER International Journal of Engineering Technology, Vol. 4, No.1 , pp. 115-140, 2016.

[4] M.F.Othmana, K.Shazali, Wireless Sensor Network Applications: A Study in Environment Monitoring System. International Symposium on Robotics and Intelligent Sensors 2012 (IR IS 2012), pp. 1204 – 1210, 2012.

[5] Nurul Fahmi, M. Udin Harun Al Rasyid, Amang Sudarsono. Adaptive Schedulling for Health Monitoring System Based on the IEEE 802.15.4 Sleep Standart. EMITTER International Journal of Engineering Technology, Vol. 4, No.1 , pp. 91-114, 2016.

[6] J.Bethencourt, A.Sahai, and B.Waters, Ciphertext-policy Attribute-Based Encryption. IEEE Symposium on Security and Privacy. pp. 321-334, 2007.

[7] J.Benthencourt, A.Sahai, and B.Waters. cpabe toolkit in advanced Crypto Software Collection.[Online].From:http://hms.isi.jhu.edu/acsc/cpabe. [accessed on Oktober 2015].

[8] B.Lynn. PBC (Pairing-Based Cryptography) library. [Online]. From: http://crypto.stanford.edu/pbc. [accessed on Oktober 2015].

[9] S. Roy, M. Chuah. Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) System for the DTNs. Journal of Cryptology, vol. 17, No.4, pp.297-319,2004.

[10] Samsul Huda, Nurul Fahmi, Amang Sudarsono, and M. Udin Harun Al Rasyid, "Secure Data Sensor Sharing on Ubiquitous Environmental Health Monitoring Application", Jurnal Teknologi (Sciences & Engineering) 78:6-3 (2016), pp. 53-58, 2016.

[11] J.H. Chen, Y.T.Wang, and K. Chen, Attribute-Based Key-Insulated Encryption, Journal of Information Science and Engineering, Vol.27, pp. 437–449, 2011.

[12] W. Stalling, Network Security Essentials: Applications and Standards, Prentice Hall Press, 4th edition, ISBN-13: 978-0136108054, 2010.

[13] J.H. Chen, Y.T.Wang, and K. Chen, Attribute-Based Key-Insulated Encryption,Journal of Information Science and Engineering, Vol.27, pp.437-449, 2011.

[14] H. Kwon, D. Kim, C. Hahn, and J. Hur, Secure Authentication using Ciphertext Policy Attribute-Based Encryption in Mobile Multi-hop Networks,Multimedia Tools and Applications, pp.1-15, 2016.

[15] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker,"Mediated Ciphertext-Policy Attribute-Based Encryption and ItsApplication," Proc. Int'l Workshop Information Security Applications (WISA '09), pp. 309-323, 2009.

[16] Koo, D., Hur, J., and Yoon, H. "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage.", Computers & Electrical Engineering, vol 39, no1, pp 34-46, 2013.

[17] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,"Proc. ACM Conf.Computer and Comm. Security, pp. 121-130, 2009.

[18] A. Lewko, A Sahai and B Waters, "Revocation Systems with Very Small Private Keys". IEEE Symposium on Security and Privacy 2010, pp. 273-285, 2010.

[19] L. Touati, Y. Challal and A. Bouabdallah, "Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things", Internationan Conference on Advanced Networking, Distributed System and Aplications. pp.64-69, 2014.