IV. CONCLUSIONS

We implementation CP-ABE with combining a timestamp digital signature using RSA 2048 to sign and verify the data, the timestamp digital signature will provide data integrity and give a guarantee the authenticity of data that has been sent. Our system can secure the data information and give the guarantee to the data information will not change during the process from the data center until the user received the data, we provide the guarantee the user will not receive a fake data. The combination between CP-ABE to secure the data with encryption and decryption process to protect the data sensor, to revoke the user did the illegal access and timestamp digital signature with RSA 2048 in the data is not affecting to performance of the system. Our experimental show the results all of process less than 3 second with 1000 number of revoked users.

REFERENCES

[1] 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.

[2] M. Udin Harun Al Rasyid, Achmad SayfudinAchmad Sayfudin, Arif Basofi, Amang Sudarsono. Development of Semantic Sensor Web for Monitoring Environment Conditions. International Seminar on Intelligent Technology and Its Applications (ISITIA),pp. 607-612, 2016.

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

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

[5] Munsyi, Amang Sudarsono, and M.U.H. Al Rasyid, "Secure Data Sensor In Environmental Monitoring System Using Attribute-Based Encryption With Encryption", International Journal on Advanced Science, Engineering and Information Technology, Vol 7, pp., 2017.

[6] A.Sudarsono, M.Udin Harun 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, 2016.*

[7] Munsyi, Amang Sudarsono, M. Udin Harun Al Rasyid, "Secure Data Sensor Access Using Attribute-Based Encryption With Revocation Environmental Monitoring", Knowledge Creation & Intelligent Computing (KCIC), pp. 73-79, 2016.

[8] K. H. Patel, S.S Patel. 2016, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" International Journal for Scientific Research & Development, vol. 4, pp.543-548, 2016.

[9] 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 2016].

[10] B.Lynn. PBC (Pairing-Based Cryptography) library. [Online]. From: http://crypto.stanford.edu/pbc. [accessed on Oktober 2016].

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.