continue to emerge from time to time, so the IoT security protocol shall evolve to deal with the new threats.

REFERENCES

[1] Ahmad J, Zafar F, "Review of body area network technology & wireless medical monitoring." *International Journal of Information and Communication Technology. 2(2).*, 2012.

[2] Yadav G, Devi HMS., "Arduino based Security System – An Application of IOT", International Journal of Engineering Trends and Technology (IJETT) – Special Issue. pp. 209–212. 2017.

[3] Wahjuni S, Maarik A, Budiardi T. "The Fuzzy Inference System for Intelligent Water Quality Monitoring System to Optimize Eel Fish Farming", *Proceeding of The International Symposium on Electronics and Smart Devices. Bandung (ID)*, 2016.

[4] Wahjuni S, Waladi A. "Komiot: Exploring Rest Protocol for IoT Server of The Automatic Control System for Production Land Irrigation.", *Proceedings of The 4th International Seminar on Sciences "Sciences for Green Development" pp.71-81.,* 2017

[5] (2018) ESET We Live Security Website [Online]. Available: https://www.welivesecurity.com/2018/03/02/start-analyzing-security-iot-devices/

[6] Loi F, Sivanathan A, Gharakheili HH, Radford A, Sivaraman, V. "Systematically evaluating security and privacy for consumer IoT devices", *In Proceedings of the 2017 Workshop on Internet of Things Security and Privacy (pp. 1-6)*, 2017.

[7] Wu W, Zhang L. "LBlock: a lightweight block cipher". *International Conference on Applied Cryptography and Network Security (pp. 327-344). Berlin(DE): Springer*, 2011.

[8] Dinu D, Le Corre Y, Khovratovich D, Perrin L, Großschädl J, Biryukov A, "Triathlon of lightweight block ciphers for the internet of things*", Journal of Cryptographic Engineering. pp.1-20.*, 2015.

[9] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B. and Wingers, L. "The SIMON and SPECK block ciphers on AVR 8-bit microcontrollers". *In International Workshop on Lightweight Cryptography for Security and Privacy (pp. 3-20). Springer, Cham.*, 2014

[10] Beaulieu R., Treatman-Clark S, Shors D, Weeks B, Smith J, Wingers L., "The SIMON and SPECK lightweight block ciphers". *52nd ACM/EDAC/IEEE Design Automation Conference (DAC) (pp. 1-6).,* 2015.

[11] Biryukov A, Dinu D, Großschädl J., "Correlation power analysis of lightweight block ciphers: from theory to practice"., *In International Conference on Applied Cryptography and Network Security. (pp. 537-557)*, 2016.

[12] Dinur, I. "Improved differential cryptanalysis of round-reduced speck". *In International Conference on Selected Areas in Cryptography (pp. 147-164). Springer, Cham*. 2014

[13] Dwivedi, A.D., Morawiecki, P. and Srivastava, G. "Differential cryptanalysis of round-reduced SPECK suitable for internet of things devices". *IEEE Access, 7, pp.16476-16486.*, 2019

[14] Fu, K., Wang, M., Guo, Y., Sun, S. and Hu, L. "MILP-based automatic search algorithms for differential and linear trails for SPECK". *In International Conference on Fast Software Encryption (pp. 268-288). Springer, Berlin, Heidelberg.* 2016, March.

[15] Aumasson, J.P., Neves, S., Wilcox-O'Hearn, Z. and Winnerlein, C., "BLAKE2: simpler, smaller, fast as MD5". *In International Conference on Applied Cryptography and Network Security (pp. 119-135). Springer, Berlin, Heidelberg.* 2013, June

[16] Jain, A.K., Jones, R. and Joshi, P.. "Survey of Cryptographic Hashing Algorithms for Message Signing". *Int. J. Comput. Sci. Technol, 8, pp.18-22.* , 2017

[17] Luykx, A., Mennink, B. and Neves, S. "Security analysis of BLAKE2's modes of operation." *IACR Transactions on Symmetric Cryptology, pp.158-176.*`, 2016

[18] Bin-Rabiah A, Ramakrishnan KK, Liri E, Kar K. "A Lightweight Authentication and Key Exchange Protocol for IoT". *Workshop on Decentralized IoT Security and Standards (DISS). San Diego(US)*, 2018.