DAFTAR PUSTAKA

[1] Panda, Madhumita. (2015). *Data Security in Wireless Sensor Network via AES Algorithm.* ISCO. India

[2] Maphats'oe, Ts'itso dan Muthoni Masinde. (2016). *A security Algorithm for Wireless Sensor Networks in the Internet of Things Paradigm.*IST-Africa.South Africa

[3] Yang, Bin. (2009). *Study on Security of Wireless Sensor Network Based on ZigBee Standard.* International Conference Computational Intelligence and *Security*. China

[4] Dini, Gianluca dan Marco Tiloca. (2010). *Considerations on Security in ZigBee Networks.*International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing. Italia

[5] Granjal, Jorje., Edmundo Monteiro, dan Jorge Sa Silva. (2015). *Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues.* IEEE Communications Surveys and Tutorials

[6] Candra, Shalahuddin Kartika. "Desain dan Implementasi WSN pada Tempat Sampah dalama Gedung Berbasis Mikrokontroler Menggunakan RF Modul Zigbee dengan Topologi Cluster Tree". Universitas Telkom. *Band*ung. 2015

[7] Geier, Jim. *"Designing and Deploying 802.11n Wireless Networks".* Cisco Press. Indianapolis USA. 2010

[8] Masica, Ken. (2007). *Recommended Prectices Guide for Securing ZigBee Wireless Networks in Process Control System Envireonments*. DHS US CERT Control Systems *Security* Program (CSSP). Amerika Serikat

[9] Blonter, Melissa., dan Chow Ming. (2015). *Smart Home Technology : The ZigBee Protocol*. Computer Systems *Security*. Tufts University. Amerika Serikat

[10] Daemen, Joan., dan Vincent Rijmen. *"The Design of Rijndael AES – The Advanced Encryption Standard"*. Springer. Belgium. 2001

[11] Johnstone, Michael N., dan Jeremy A. Jarvis. (2011). *Penetration of ZigBee-based Wireless Sensor Networks*. Australian Information Warfare and *Security* Conference. Edith Cowan University. Australia

[12] Stelte, Bjorn., dan Gabi Dreo Rodosek. (2013). *Thwaeting Attacks on ZigBee – Removal of the KillerBee Stinger.* IFIP. Germany

[13] Soleimay, Kiana. (2011). *Security in IEEE 802.15.4/zigbee.* University of Mazandaran. Iran

[14] Olawumi, Olayemi., Keijo Haataja, Mikko Asikainen, Niko Vidgren, dan Pekka Toivanen. (2014). *Three Practical Attacks Against ZigBee Security: Attacks Scenario Definitions, Practical Experiments, Countermeasures, and Lesson Learned*. IEEE. Finlandia

[15] Digi International Inc. (2017). *"*XBee/XBee-*PRO® S2C Zigbee® RF Module"*. [Online]. Tersedia: https: //www.digi.com/resources/ documentation/DigiDocs/ 90002002/default.htm#Containers yang direkam pada 13 September 2017

[16] Riverloopsec. (2017). *"IEEE 802.15.4/ZigBee Security Research Toolkit".* [Online]. Tersedia: http://www.riverloop*security*.com yang direkam pada 20 Juni 2017

[17] J.Market, M.Massoth, K-P.Fischer-Hellmann, S.M.Furnell, dan C.Bolan. (2011). *Attack Vectors to Wireless ZigBee Network Communications – Analysis and Countermeasures*. Proceedings of SEIN. Jerman

[18] Vaccari, Ivan., Enrico Cambiaso, and Maurizio Aiello. (2017). *Remotly Exploiting AT Command Attacks on ZigBee Networks.* Hindawi. Mesir

[19] Seitz, Andrew., dan Benjamin Ramsey. (2016). *Z-Ranger : An Improved Tool Set for ZigBee Warwalking*. 11th International Conference on Cyber Warfare & *Security* Boston University. USA