DAFTAR PUSTAKA

[1] R. H. Weber, “Internet of Things – New security and privacy challenges,” *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.

[2] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, P. Doody, F. Peter, G. Patrick, G. Sergio, B. Harald, Sundmaeker Alessandro, J. Ignacio Soler, M. Margaretha, H. Mark, E. Markus, and D. Pat, “Internet of Things Strategic Research Roadmap,” 2009.

[3] S. Tozlu, M. Senel, W. Mao, and A. Keshavarzian, “Wi-Fi enabled sensors for internet of things: A practical approach,” *IEEE Commun. Mag.*, vol. 50, no. 6, pp. 134–143, 2012.

[4] J. Pescatore, “Securing the ‘ Internet of Things ’ Survey,” 2014.

[5] “IoT Privacy , Data Protection , Information Security,” pp. 1–9.

[6] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, “TRM-IoT: A trust management model based on fuzzy reputation for internet of things,” *Comput. Sci. Inf. Syst.*, vol. 8, no. 4, pp. 1207–1228, 2011.

[7] S. Zafar and M. K. Soni, “Trust based QOS protocol(TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET,” *ICROIT 2014 - Proc. 2014 Int. Conf. Reliab. Optim. Inf. Technol.*, pp. 173–177, 2014.

[8] P. Bedi and R. Sharma, “Trust based recommender system using ant colony for trust computation,” *Expert Syst. Appl.*, vol. 39, no. 1, pp. 1183–1190, 2012.

[9] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, “A subjective model for trustworthiness evaluation in the social Internet of Things,” *IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC*, pp. 18–23, 2012.

[10] Z. Chen, L. Li, and J. Gui, “Fuzzy Theory for the P2P Subject Trust Evaluation Model,” *Int. J. Adv. Comput. Technol.*, vol. 4, no. 8, pp. 67–74, 2012.

[11] Z. Yan and P. Zhang, “A Survey on Trust Management for Internet of Things,” 2014.

[12] Y. Yu, Z. Jia, W. Tao, and B. Xue, “An Efficient Trust Evaluation Scheme for

Node Behavior Detection in the Internet of Things," *Wirel. Pers. Commun.*, vol. 93, no. 2, pp. 571–587, 2017.

[13] M. Yu, H. Lin, and J. Hu, "A data trustworthiness enhanced reputation mechanism for mobile crowd sensing," in *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017*, 2018, vol. 2018–Janua, pp. 743–747.

[14] V. B. Reddy, S. Venkataraman, and A. Negi, "Communication and Data Trust for Wireless Sensor Networks Using D-S Theory," *IEEE Sens. J.*, vol. 17, no. 12, pp. 3921–3929, 2017.

[15] J. Yuan and X. Li, "A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion," *IEEE Access*, vol. 6, 2018.

[16] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," *IEEE Comput. Soc.*, vol. 44, no. 9, pp. 51–58, 2011.

[17] V. Suryani, S. Sulistyo, and Widyawan, "A Performance Comparison of OpenMTC Platform," in *International Conference on Science and Technology 2015*, 2015.

[18] Y. SONG, "Security in Internet of Things," Royal Institute of Technology, 2013.

[19] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "Ad Hoc Networks DTLS based security and two-way authentication for the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710–2723, 2013.

[20] L. Veltri, S. Cirani, S. Busanelli, and G. Ferrari, "A novel batch-based group key management protocol applied to the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2724–2737, 2013.

[21] N. Ye, Y. Zhu, R. C. Wang, R. Malekian, and Q. M. Lin, "An efficient authentication and access control scheme for perception layer of internet of things," *Appl. Math. Inf. Sci.*, vol. 8, no. 4, pp. 1617–1624, 2014.

[22] K. Fan, J. Li, H. Li, X. Liang, X. Shen, and Y. Yang, "ESLRAS: A lightweight

RFID authentication scheme with high efficiency and strong security for internet of things," in *Proceedings of the 2012 4th International Conference on Intelligent Networking and Collaborative Systems, INCoS 2012*, 2012, pp. 323–328.

[23] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, "Towards viable certificate-based authentication for the internet of things," *Proc. 2nd ACM Work. Hot Top. Wirel. Netw. Secur. Priv. - HotWiSec '13*, p. 37, 2013.

[24] S. A. Ch, N. Uddin, M. Sher, A. Ghani, H. Naqvi, and A. Irshad, "An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography," *Multimed. Tools Appl.*, pp. 1711–1723, 2014.

[25] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014.

[26] R. Hummen, H. Shafagh, and S. Raza, "Delegation-based Authentication and Authorization for the IP-based Internet of Things," in *IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2014, pp. 284–292.

[27] V. Suryani, S. Sulistyo, and Widyawan, "Penggunaan Distribusi Kunci Diffie-Hellman untuk Penerapan Aspek Privacy pada Automatic Meter Reading (AMR)," in *The 7th Conference on Information Technology and Electrical Engineering (CITEE)*, 2015, pp. 1–5.

[28] F. Bao and I.-R. Chen, "Dynamic trust management for internet of things applications," in *Proceedings of the 2012 international workshop on Self-aware internet of things - Self-IoT '12*, 2012, p. 1.

[29] N. Oualha and K. T. Nguyen, "Lightweight attribute-based encryption for the internet of things," *2016 25th Int. Conf. Comput. Commun. Networks, ICCCN 2016*, 2016.

[30] L. Touati, Y. Challal, and A. Bouabdallah, "C-CP-ABE: Cooperative ciphertext policy attribute-based encryption for the internet of things," *Proc. - 2014 Int. Conf. Adv. Netw. Distrib. Syst. Appl. INDS 2014*, pp. 64–69, 2014.

[31] J. Su, D. Cao, B. Zhao, X. Wang, and I. You, "ePASS : An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 33, pp. 11–18, 2014.

[32] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT target-driven applications," *Comput. Secur.*, vol. 37, pp. 111–123, 2013.

[33] Xin Huang, Rong Fu, Bangdao Chen, Tingting Zhang, A. W. W. Roscoe, X. Huang, R. Fu, B. Chen, T. Zhang, and A. W. W. Roscoe, "User interactive Internet of things privacy preserved access control," *Proc. 2012 Int. Conf. Internet Technol. Secur. Trans.*, pp. 597–602, 2012.

[34] V. Suryani, S. Sulistyo, and W. Widyawan, "Internet of Things (IoT) Framework for Granting Trust among Objects," *J. Inf. Process. Syst.*, vol. 13, no. 6, pp. 1613–1627, 2017.

[35] V. Suryani, S. Sulistyo, and Widyawan, "Trust-Based Privacy for Internet of Things," *IJECE*, 2016.

[36] V. Suryani, S. Sulistyo, and W. Widyawan, "ConTrust : A Trust Model to Enhance The Privacy in Internet of Things," *Int. J. Intell. Eng. Syst.*, vol. 10, no. 3, pp. 1–8, 2017.

[37] V. Suryani, S. Sulistyo, and W. Widyawan, "Simulation of trust-based attacks in Internet of Things," in *MATEC Web of Conferences*, 2018, vol. 154, pp. 2–5.

[38] V. Suryani, S. Sulistyo, and W. Widyawan, "Two - phase Security Protection for Internet of Things," 2018.

[39] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," *Int. Conf. Wirel. Mob. Comput. Netw. Commun.*, pp. 600–607, 2013.

[40] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 5, pp. 763–771, 2014.

[41] D. Thatmann, S. Zickau, A. Forster, and A. Kupper, "Applying Attribute-Based Encryption on Publish Subscribe Messaging Patterns for the Internet of Things," *Proc. - 2015 IEEE Int. Conf. Data Sci. Data Intensive Syst. 8th IEEE Int. Conf.*

Cyber, Phys. Soc. Comput. 11th IEEE Int. Conf. Green Comput. Commun. 8th IEEE Inte, pp. 556–563, 2015.

[42] D. Evans and D. M. Eyers, “Efficient data tagging for managing privacy in the Internet of Things,” *Proc. - 2012 IEEE Int. Conf. Green Comput. Commun. GreenCom 2012, Conf. Internet Things, iThings 2012 Conf. Cyber, Phys. Soc. Comput. CPSCom 2012*, pp. 244–248, 2012.

[43] S. Alanazi, J. Al-Muhtadi, A. Derhab, K. Saleem, A. N. Alromi, H. S. Alholaibah, and J. J. P. C. Rodrigues, “On resilience of Wireless Mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications,” *2015 17th Int. Conf. E-Health Networking, Appl. Serv. Heal. 2015*, pp. 205–210, 2016.

[44] I.-R. Chen and J. Guo, “Dynamic Hierarchical Trust Management of Mobile Groups and Its Application to Misbehaving Node Detection,” in *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, 2014, pp. 49–56.

[45] J.-H. Cho, A. Swami, and I.-R. Chen, “Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks,” *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 1001–1012, 2012.

[46] F. Bao, I.-R. Chen, and J. Guo, “Scalable , Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems,” in *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, 2013.

[47] Y. Ma, H. Lu, Z. Gan, and Y. Zhao, “Trust inference path search combining community detection and ant colony optimization,” in *15th International Conference, WAIM 2014*, 2014, vol. 8485 LNCS, pp. 687–698.

[48] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno, “A decentralized approach for security and privacy challenges in the Internet of Things,” in *2014 IEEE World Forum on Internet of Things, WF-IoT 2014*, 2014, pp. 67–72.

[49] J. Duan, D. Gao, D. Yang, C. H. Foh, and S. Member, “An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications,” vol. 1, no. 1, pp. 58–69, 2014.

[50] G. Schryen, M. Volkamer, S. Ries, and S. M. Habib, "A Formal Approach Towards Measuring Trust in Distributed Systems," pp. 1739–1745, 2011.

[51] M. Anuar, M. Isa, N. N. Mohamed, H. Hashim, S. Farid, S. Adnan, J. A. Manan, and R. Mahmod, "A Lightweight and Secure TFTP Protocol for Smart Environment," no. Iscaie, pp. 302–306, 2012.

[52] A. Mana, H. Koshutanski, and E. J. Perez, "A trust negotiation based security framework for service provisioning in load-balancing clusters," *Comput. Secur.*, vol. 1, no. Elsevier, pp. 4–25, 2011.

[53] W. U. Qiu-xin, "Secure solution of trusted Internet of things base on TCM," *J. China Univ. Posts Telecommun.*, vol. 20, no. December, pp. 47–53, 2013.

[54] K. Kai, P. Zhi-bo, and W. Cong, "Security and privacy mechanism for health internet of things," *J. China Univ. Posts Telecommun.*, vol. 20, no. December, pp. 64–68, 2013.

[55] Z. Yan, W. Ding, V. Niemi, and A. V Vasilakos, "Two Schemes of Privacy-Preserving Trust Evaluation," *Futur. Gener. Comput. Syst.*, 2015.

[56] X. Xu, N. Bessis, and J. Cao, "An Autonomic Agent Trust Model for IoT systems," vol. 21, pp. 107–113, 2013.

[57] S. Tan, X. Li, and Q. Dong, "Trust based routing mechanism for securing OSLR-based MANET," *Ad Hoc Networks*, vol. 30, no. 2015, pp. 84–98, 2015.

[58] Y. Ben, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things : A context-aware and multi- service approach," *Comput. Secur.*, vol. 39, pp. 351–365, 2013.

[59] A. Samani, H. H. Ghenniwa, and A. Wahaishi, "Privacy in Internet of Things : A Model and Protection Framework," in *Procedia Computer Science*, 2015, vol. 52, pp. 606–613.

[60] R. Neisse, G. Steri, I. N. Fovino, and G. Baldini, "SecKit : A Model-based Security Toolkit for the Internet of Things," *Comput. Secur.*, vol. 54, pp. 60–76, 2015.

[61] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 49, pp. 104–112, 2015.

[62] S. Sahraoui and A. Bilami, “Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things,” *Comput. Networks*, vol. 91, pp. 26–45, 2015.

[63] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, and K. Wehrle, “A comprehensive approach to privacy in the cloud-based Internet of,” *Futur. Gener. Comput. Syst.*, 2015.

[64] M. Vucinic´, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, “OSCAR : Object security architecture for the Internet of Things,” *Ad Hoc Networks*, vol. 32, pp. 3–16, 2015.

[65] S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, and H. Tenhunen, “SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways,” *Procedia Comput. Sci.*, vol. 52, no. 0, pp. 452–459, 2015.

[66] Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, “Lightweight collaborative key establishment scheme for the Internet of Things,” *Comput. Networks*, vol. 64, pp. 273–295, 2014.

[67] H. Nasiraee and J. B. Mohasefi, “A new three party key establishment scheme: Applicable for internet-enabled sensor networks,” *Comput. Electr. Eng.*, vol. 44, no. September 2013, pp. 172–183, 2014.

[68] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, “An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment,” *Ad Hoc Networks*, no. December, 2015.

[69] D. He and S. Zeadally, “An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography,” *IEEE INTERNET THINGS J.*, vol. 2, no. 1, pp. 72–83, 2015.

[70] K. T. Nguyen, M. Laurent, and N. Oualha, “Survey on secure communication protocols for the Internet of Things,” *Ad Hoc Networks*, vol. 32, no. February, pp. 17–31, 2015.

[71] E. Rescorla, “RFC 2631: Diffie-Hellman Key Agreement Method,” 1999.

[72] M. Friedl, N. Provos, and W. Simpson, “RFC 4419 Diffie-Hellman Group

Exchange for the Secure Shell (SSH) Transport Layer Protocol," 2006.

[73] R. Shirey, "RFC 2828: Internet Security Glosary," 2000.

[74] Y. Cheng, M. Naslund, G. Selander, and E. Fogelström, "Privacy in machine-to-machine communications A state-of-the-art survey," in *2012 IEEE International Conference on Communication Systems, ICCS 2012*, 2012, pp. 75–79.

[75] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, "A systemic approach for IoT security," pp. 351–355, 2013.

[76] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, *Internet of Things Security: a top-down survey*. 2018.

[77] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," in *2016 3rd International Conference on Electronic Design (ICED)*, 2016, pp. 321–326.

[78] S. Ries, J. Kangasharju, and M. Mühlhäuser, "A Classification of Trust Systems," *Move to Meaningful Internet Syst. 2006*, pp. 894–903, 2006.

[79] D. Gambetta, *Trust: Making and Breaking Cooperative Relations*. 2000.

[80] G. Piolle, "Trust management formal techniques and systems," 2010, no. december, pp. 1–17.

[81] Y. Liu, Z. Chen, F. Xia, X. Lv, and F. Bu, "A Trust Model Based on Service Classification in Mobile Services," *Green Comput. Commun. (GreenCom), 2010 IEEE/ACM Int'l Conf. Int'l Conf. Cyber, Phys. Soc. Comput.*, pp. 1–5, 2010.

[82] H. S. G. S and S. M. Praveena, "A Survey of Futuristic Approach on Smart Agriculture Technologies Using Internet of Things," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 7, no. 3, pp. 73–77, 2017.

[83] Z. Safdar, S. Farid, M. Pasha, and K. Safdar, "A Security Model for IoT based Systems," *Tech. Journal, Univ. Eng. Technol.*, vol. 22, no. 4, pp. 74–84, 2017.

[84] R. Kaur, N. Kaur, and S. K. Sood, "Security in IoT network based on stochastic game net model," *Int. J. Netw. Manag.*, vol. 27, no. 4, pp. 1–19, 2017.

[85] J. Duan, D. Gao, C. H. Foh, and H. Zhang, "TC-BAC: A trust and centrality degree based access control model in wireless sensor networks," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2675–2692, 2013.

[86] B. Verbrugge, “Best Practice, Model, Framework, Method, Guidance, Standard: towards a consistent use of terminology – revised.” Van Haren Publishing, pp. 1–5, 2018.

[87] Z. A. Hasibuan, *Metodologi Penelitian Pada Bidang Ilmu Komputer Dan Teknologi Informasi*. Fasilkom Universitas Indonesia, 2007.

[88] L. Atzori, A. Iera, and G. Morabito, “SIoT: Giving a social structure to the internet of things,” *IEEE Commun. Lett.*, vol. 15, no. 11, pp. 1193–1195, 2011.

[89] Vera Suryani, Selo, and Widyawan, “A survey on trust management for Internet of Things,” in *International Conference on Information Technology and Electrical Engineering (ICITEE)*, 2016.

[90] H. Yoshinaga, T. Tsuchiya, and K. Koyanagi, “Coordinator election using the object model in P2P networks,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 3601 LNAI, pp. 161–172, 2005.

[91] S. H. Park, S. C. Yoo, and B. K. Kim, “An election protocol based on group membership detection algorithm in mobile ad hoc distributed systems,” *J. Supercomput.*, vol. 74, no. 5, pp. 2239–2253, 2018.

[92] A. S. Tanenbaum, *Computer Networks*, vol. 52, no. 169. 2003.

[93] W. P. Wang, “A fuzzy linguistic computing approach to supplier evaluation,” *Appl. Math. Model.*, vol. 34, no. 10, pp. 3130–3141, 2010.

[94] J. D. Bokefode, A. S. Bhise, P. A. Satarkar, and D. G. Modani, “Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption,” *Procedia Comput. Sci.*, vol. 89, pp. 43–50, 2016.

[95] A. Patil, G. Bansod, and N. Pisharoty, “Hybrid lightweight and robust encryption design for security in IoT,” *Int. J. Secur. its Appl.*, vol. 9, no. 12, pp. 85–98, 2015.

[96] Y. Mao, J. Li, M. R. Chen, J. Liu, C. Xie, and Y. Zhan, “Fully secure fuzzy identity-based encryption for secure IoT communications,” *Comput. Stand. Interfaces*, vol. 44, pp. 117–121, 2016.

[97] J. Zhang, Z. Zhou, H. Yao, Y. Zhou, and K. S. Kwak, “A novel non-cooperative power control game for cognitive radio networks,” in *Communications and*

Information Technology, ISCIT 9th International Symposium on, 2009, pp. 115–118.

[98] F. Wu and L. Xu, “A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security,” *J. Ambient Intell. Humaniz. Comput.*, vol. 8, no. 1, pp. 101–116, 2017.