DAFTAR PUSTAKA

[1] V. E. Satya, "Kajian Singkat Terhadap Isu Aktual Dan Strategis Strategi Indonesia Menghadapi Industri 4.0," *Pusat Penelitian Badan Keahlian DPR RI*, vol. X, no. 09, p. 19, 2018.

[2] R. J. Vetter, "Internet Kiosk- Computer-Controlled Devices Reach the Internet," *Computer (Long Beach Calif)*, vol. 28, no. 12, p. 66, Dec. 1995, doi: 10.1109/MC.1995.476201.

[3] Project CASAGRAS, "CASAGRAS Final Report: RFID and the Inclusive Model for the Internet of Things," *Sci Am*, vol. 291, no. 4, pp. 10–12, 2009, doi: 10.1038/scientificamerican1004-76.

[4] H. S. G. S and S. M. Praveena, "A Survey of Futuristic Approach on Smart Agriculture Technologies Using Internet of Things," *International Journal of Emerging Technology and Advanced Engineering*, vol. 7, no. 3, pp. 73–77, 2017.

[5] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer (Long Beach Calif)*, vol. 44, no. 9, pp. 51–58, Sep. 2011, doi: 10.1109/MC.2011.291.

[6] C. Maple, "Security and privacy in the internet of things," *Journal of Cyber Policy*, vol. 2, no. 2, pp. 155–184, 2017, doi: 10.1080/23738871.2017.1366536.

[7] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," 2015, *Elsevier B.V.* doi: 10.1016/j.comnet.2014.11.008.

[8] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for Internet of Things," in *2014 International Symposium on Next-Generation Electronics (ISNE)*, IEEE, 2014, pp. 1–2. doi: 10.1109/ISNE.2014.6839375.

[9] S. Janbabaei, H. Gharaee, and N. Mohammadzadeh, "Lightweight, anonymous and mutual authentication in IoT infrastructure," in *2016 8th International Symposium on Telecommunications (IST)*, IEEE, Sep. 2016, pp. 162–166. doi: 10.1109/ISTEL.2016.7881802.

[10] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An Efficient Distributed Trust Model for Wireless Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1228–1237, 2015, doi: 10.1109/TPDS.2014.2320505.

[11] V. Suryani, Selo, and Widyawan, "A survey on trust in Internet of Things," *2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)*, vol. 42, pp. 1–6, 2016, doi: 10.1109/ICITEED.2016.7863238.

[12] J. Guo, I. R. Chen, and J. J. P. Tsai, "A survey of trust computation models for service management in internet of things systems," *Comput Commun*, vol. 97, pp. 1–14, 2017, doi: 10.1016/j.comcom.2016.10.012.

[13] I. R. Chen, J. Guo, and F. Bao, "Trust Management for SOA-Based IoT and Its Application to Service Composition," *IEEE Trans Serv Comput*, vol. 9, no. 3, pp. 482–495, 2016, doi: 10.1109/TSC.2014.2365797.

[14] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness Management in the Social Internet of Things," *IEEE Trans Knowl Data Eng*, vol. 26, no. 5, pp. 1253–1266, 2014, doi: 10.1109/TKDE.2013.105.

[15] C. Marche and M. Nitti, "Trust-Related Attacks and Their Detection: A Trust Management Model for the Social IoT," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3297–3308, 2021, doi: 10.1109/TNSM.2020.3046906.

[16] I. R. Chen and J. Guo, "Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection," in *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 2014, pp. 49–56. doi: 10.1109/AINA.2014.13.

[17] S. Javanmardi, M. Shojafar, S. Shariatmadari, and S. S. Ahrabi, "FR trust: A fuzzy reputation-based model for trust management in semantic P2P grids," *International Journal of Grid and Utility Computing*, vol. 6, no. 1, pp. 57–66, 2015, doi: 10.1504/IJGUC.2015.066397.

[18] Z. Yan, P. Zhang, and A. V Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014, doi: 10.1016/j.jnca.2014.01.014.

[19] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social Internet of Things," in *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*, Sydney: IEEE, Sep. 2012, pp. 18–23. doi: 10.1109/PIMRC.2012.6362662.

[20] L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a social structure to the internet of things," *IEEE Communications Letters*, vol. 15, no. 11, pp. 1193–1195, 2011, doi: 10.1109/LCOMM.2011.090911.111340.

[21] I. R. Chen and J. Guo, "Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection," in *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 2014, pp. 49–56. doi: 10.1109/AINA.2014.13.

[22] S. Zafar and M. K. Soni, "Trust based QOS protocol(TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET," *ICROIT 2014 - Proceedings of the 2014 International Conference on Reliability, Optimization and Information Technology*, pp. 173–177, 2014, doi: 10.1109/ICROIT.2014.6798315.

[23] Y. Ma, H. Lu, Z. Gan, and Y. Zhao, "Trust Inference Path Search Combining Community Detection and Ant Colony Optimization," Springer Verlag, 2014, pp. 687–698. doi: 10.1007/978-3-319-08010-9_73.

[24] 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," *Computer Science and Information Systems*, vol. 8, no. 4, pp. 1207–1228, 2011, doi: 10.2298/CSIS110303056C.

[25] J. Duan, D. Gao, D. Yang, C. H. Foh, and H. H. Chen, "An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications," *IEEE Internet Things J*, vol. 1, no. 1, pp. 58–69, Feb. 2014, doi: 10.1109/JIOT.2014.2314132.

[26] 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)*, IEEE, Mar. 2013, pp. 1–7. doi: 10.1109/ISADS.2013.6513398.

[27] V. Suryani, S. Sulistyo, and Widyawan, "Trust-based privacy for internet of things," *International Journal of Electrical and Computer Engineering*, vol. 6, no. 5, pp. 2396–2402, 2016, doi: 10.11591/ijece.v6i5.9678.

[28] V. Suryani, S. Sulistyo, and Widyawan, "Internet of Things (IoT) Framework for Granting Trust among Objects," *Journal of Information Processing Systems*, vol. 13, no. 6, pp. 1613–1627, 2017, doi: 10.3745/JIPS.03.0088.

[29] V. Suryani, S. Sulistyo, and W. Widyawan, "ConTrust: A trust model to enhance the privacy in internet of things," *International Journal of Intelligent Engineering and Systems*, vol. 10, no. 3, pp. 30–37, 2017, doi: 10.22266/ijies2017.0630.04.

[30] 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, doi: 10.1016/j.adhoc.2013.05.005.

[31] Y. B Saied, 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, no. PART B, pp. 351–365, 2013, doi: 10.1016/j.cose.2013.09.001.

[32] S. Joshi and D. K. Mishra, "A roadmap towards trust management & privacy preservation in mobile ad hoc networks," *Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016*, 2017, doi: 10.1109/ICTBIG.2016.7892714.

[33] A. Bhargava, S. Verma, B. K. Chaurasia, and G. S. Tomar, "Computational trust model for Internet of Vehicles," *2017 Conference on Information and Communication Technology, CICT 2017*, vol. 2018-April, pp. 1–5, 2018, doi: 10.1109/INFOCOMTECH.2017.8340600.

[34] J. Caminha, A. Perkusich, and M. Perkusich, "A smart middleware to perform semantic discovery and trust evaluation for the Internet of Things," *CCNC 2018 - 2018 15th IEEE Annual Consumer Communications and Networking Conference*, vol. 2018-Janua, pp. 1–2, 2018, doi: 10.1109/CCNC.2018.8319287.

[35] U. Jayasinghe, G. M. Lee, T.-W. Um, and Q. Shi, "Machine Learning based Trust Computational Model for IoT Services," *IEEE Transactions on Sustainable Computing*, vol. 3782, no. c, p. 1, 2018, doi: 10.1109/TSUSC.2018.2839623.

[36] J. Wang, H. Wang, H. Zhang, and N. Cao, "Trust and Attribute-Based Dynamic Access Control Model for Internet of Things," *Proceedings - 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2017*, vol. 2018-Janua, pp. 342–345, 2018, doi: 10.1109/CyberC.2017.47.

[37] 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, pp. 23626–23638, 2018, doi: 10.1109/ACCESS.2018.2831898.

[38] A. Favier, L. Arantes, J. Lejeune, and P. Sens, "Centrality-Based Eventual Leader Election in Dynamic Networks," *2021 IEEE 20th International Symposium on Network Computing and Applications, NCA 2021*, 2021, doi: 10.1109/NCA53618.2021.9685390.

[39] T. Khan *et al.*, "An efficient trust-based decision-making approach for WSNs: Machine learning oriented approach," *Comput Commun*, vol. 209, pp. 217–229, 2023, doi: https://doi.org/10.1016/j.comcom.2023.06.014.

[40] M. A. Iqbal, O. G. Olaleye, and M. A. Bayoumi, "A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches," *Global Journal of Computer Science and Technology: E Network, Web & Security*, vol. 16, no. 7, 2016.

[41] R. Minerva, A. Biru, and D. Rotondi, "Toward a definition of the Internet of Things," 2015, *IEEE*.

[42] K. K. Patel, S. M. Patel, and P. G. Scholar, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges," *International Journal of Engineering Science and Computing*, vol. 6, no. 5, pp. 1–10, 2016, doi: 10.4010/2016.1482.

[43] M. M. Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," *Proceedings of the IEEE International Conference on VLSI Design*, pp. 203–208, 2013, doi: 10.1109/VLSID.2013.222.

[44] A. M. Nia, S. Member, and M. Mozaffari-kermani, "Energy-Efficient Long-term Continuous Personal Health Monitoring," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 85–98, 2015, doi: 10.1109/TMSCS.2015.2494021.

[45] P. Alinia, R. Saeedi, R. Fallahzadeh, A. Rokni, and H. Ghasemzadeh, "A Reliable and Reconfigurable Signal Processing Framework for Estimation Metabolic Equivalent of Task in Wearable Sensors," *IEEE J Sel Top Signal Process*, vol. 10, no. 5, p. 1, 2016, doi: 10.1109/JSTSP.2016.2569472.

[46] K. Su, J. Li, and H. Fu, "Smart city and the applications," *2011 International Conference on Electronics, Communications and Control, ICECC 2011 - Proceedings*, pp. 1028–1031, 2011, doi: 10.1109/ICECC.2011.6066743.

[47] M. T. Lazarescu, "Design of a WSN Platform for Long-Term Environmental Monitoring for IoT Applications," *IEEE J Emerg Sel Top*

Circuits Syst, vol. 3, no. 1, pp. 45–54, Mar. 2013, doi: 10.1109/JETCAS.2013.2243032.

[48] R. P. Grimaldi, *Discrete and Combinatorial Mathematics: an Applied Introduction*. Boston: Pearson Addison Wesley, 2004.

[49] M. Tsvetovat and A. Kouznetsov, *Social Network Analysis for Startup*. Cambridge: OReilly Media, 2011.

[50] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer (Long Beach Calif)*, vol. 44, no. 9, pp. 51–58, Sep. 2011, doi: 10.1109/MC.2011.291.

[51] C. Maple, "Security and privacy in the internet of things," *Journal of Cyber Policy*, vol. 2, no. 2, pp. 155–184, 2017, doi: 10.1080/23738871.2017.1366536.

[52] H. Salmani, M. M. Tehranipoor, and S. Member, "Vulnerability Analysis of a Circuit Layout to Hardware Trojan Insertion," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1214–1225, 2016, doi: 10.1109/TIFS.2016.2520910.

[53] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Trans Emerg Top Comput*, vol. 5, no. 4, pp. 586–602, Oct. 2017, doi: 10.1109/TETC.2016.2606384.

[54] T. Martin, M. Hsiao, Dong Ha, and J. Krishnaswami, "Denial-of-service attacks on battery-powered mobile computers," in *Second IEEE Annual Conference on Pervasive Computing and Communications, 2004. Proceedings of the*, IEEE, 2004, pp. 309–318. doi: 10.1109/PERCOM.2004.1276868.

[55] F. Stajano and R. J. Anderson, "The Resurrecting Duckling: Security issues for Ad-hoc Wireless Network," in *Proceedings of the 7th International Workshop on Security Protocols*, 1999, pp. 172–194.

[56] A. Juels, "RFID security and privacy: a research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, Feb. 2006, doi: 10.1109/JSAC.2005.861395.

[57] M. Lehtonen, D. Ostojic, A. Ilic, and F. Michahelles, "Securing RFID Systems by Detecting Tag Cloning," in *Lecture Notes in Computer Science book series (LNCS, volume 5538)*, 5538th ed., Berlin: Springer Berlin Heidelberg, 2009, ch. Pervasive, pp. 291–308. doi: 10.1007/978-3-642-01516-8_20.

[58] D. N. Duc and K. Kim, "Defending RFID authentication protocols against DoS attacks," *Comput Commun*, vol. 34, no. 3, pp. 384–390, Mar. 2011, doi: 10.1016/j.comcom.2010.06.014.

[59] J. P. Walters and Z. Liang, "Wireless Sensor Network Security : A Survey," in *Security in Distributed, Grid, and Pervasive Computing*, Auerbach Publications, CRC Press, 2006, pp. 1–50.

[60] S. O. Uwagbole, W. J. Buchanan, and L. Fan, "Applied Machine Learning predictive analytics to SQL Injection Attack detection and prevention," *Proceedings of the IM 2017 - 2017 IFIP/IEEE International Symposium on Integrated Network and Service Management*, no. October, pp. 1087–1090, 2017, doi: 10.23919/INM.2017.7987433.

[61] B. Biggio, B. Nelson, and P. Laskov, "Poisoning Attacks against Support Vector Machines," *Proceedings of the 29th International Conference on Machine Learning (ICML 2012)*, Jun. 2012.
[62] B. I. P. Rubinstein *et al.*, "Stealthy poisoning attacks on PCA-based anomaly detectors," *ACM SIGMETRICS Performance Evaluation Review*, vol. 37, no. 2, p. 73, 2009, doi: 10.1145/1639562.1639592.
[63] W. Najib, S. Sulistyo, and Widyawan, "Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, vol. 9, no. 4, pp. 375–384, 2020, doi: 10.22146/jnteti.v9i4.539.
[64] N. B. Truong, H. Lee, B. Askwith, and G. M. Lee, "Toward a trust evaluation mechanism in the social internet of things," *Sensors (Switzerland)*, vol. 17, no. 6, pp. 1–24, 2017, doi: 10.3390/s17061346.
[65] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 0, pp. 1–24, 2018, doi: 10.1016/j.comnet.2018.03.012.
[66] S. Janbabaei, H. Gharaee, and N. Mohammadzadeh, "Lightweight, anonymous and mutual authentication in IoT infrastructure," in *2016 8th International Symposium on Telecommunications (IST)*, IEEE, Sep. 2016, pp. 162–166. doi: 10.1109/ISTEL.2016.7881802.
[67] Y. Cherdantseva and J. Hilton, "A reference model of information assurance & security," *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, pp. 546–555, 2013, doi: 10.1109/ARES.2013.72.
[68] W. Najib, S. Sulistyo, and Widyawan, "Survey on Trust Calculation Methods in Internet of Things," *Procedia Comput Sci*, vol. 161, pp. 1300–1307, 2019, doi: 10.1016/j.procs.2019.11.245.
[69] Z. Chen, R. Ling, C.-M. Huang, and X. Zhu, "A scheme of access service recommendation for the Social Internet of Things," *International Journal of Communication Systems*, vol. 29, no. 4, pp. 694–706, Mar. 2016, doi: 10.1002/dac.2930.
[70] S. Zafar and M. K. Soni, "Trust based QOS protocol(TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET," *ICROIT 2014 - Proceedings of the 2014 International Conference on Reliability, Optimization and Information Technology*, pp. 173–177, 2014, doi: 10.1109/ICROIT.2014.6798315.
[71] J. Duan, D. Gao, D. Yang, C. H. Foh, and H. H. Chen, "An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications," *IEEE Internet Things J*, vol. 1, no. 1, pp. 58–69, Feb. 2014, doi: 10.1109/JIOT.2014.2314132.
[72] S. Zafar and M. K. Soni, "Trust based QOS protocol(TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET," *ICROIT 2014 - Proceedings of the 2014 International Conference on Reliability, Optimization and Information Technology*, pp. 173–177, 2014, doi: 10.1109/ICROIT.2014.6798315.

[73] Y. Ma, H. Lu, Z. Gan, and Y. Zhao, "Trust Inference Path Search Combining Community Detection and Ant Colony Optimization," Springer Verlag, 2014, pp. 687–698. doi: 10.1007/978-3-319-08010-9_73.

[74] I. R. Chen, F. Bao, M. Chang, and J. H. Cho, "Trust management for encounter-based routing in delay tolerant networks," *GLOBECOM - IEEE Global Telecommunications Conference*, pp. 1–6, 2010, doi: 10.1109/GLOCOM.2010.5683235.

[75] X. Wu, "A robust and adaptive trust management system for guaranteeing the availability in the internet of things environments," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 5, pp. 2396–2413, 2018, doi: 10.3837/tiis.2018.05.026.

[76] Y. Wang, Y. Lu, I. Chen, J. Cho, A. Swami, and C. Lu, "LogitTrust : A Logit Regression-based Trust Model for Mobile Ad Hoc Networks State of the Art," *Proceedings of the 6th ASE International Conference on Privacy, Security, Risk and Trust (PASSAT '14)*, 2014.

[77] U. Jayasinghe, G. M. Lee, T.-W. Um, and Q. Shi, "Machine Learning Based Trust Computational Model for IoT Services," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 39–52, 2018, doi: 10.1109/tsusc.2018.2839623.

[78] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning," pp. 1–20, Jan. 2018.

[79] I. R. Chen, F. Bao, M. Chang, and J. H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, 2014, doi: 10.1109/TPDS.2013.116.

[80] Y. Liu, Z. Chen, F. Xia, X. Lv, and F. Bu, "A trust model based on service classification in mobile services," *Proceedings - 2010 IEEE/ACM International Conference on Green Computing and Communications, GreenCom 2010, 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing, CPSCom 2010*, pp. 572–576, 2010, doi: 10.1109/GreenCom-CPSCom.2010.19.

[81] C. E. Dawson, *Projects in Computing and Information Systems A Student's Guide*, 3rd ed. Edinburg: Pearson Education Limited, 2005.

[82] W. Najib, S. Sulistyo, and Widyawan, "Trust Based Security Model in IoT Ecosystem," *6th International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)*, 2022.

[83] W. Najib, S. Sulistyo, and Widyawan, "QS-Trust: An IoT ecosystem security model incorporating quality of service and social factors for trust assessment," *Communications in Science and Technology*, vol. 9, no. 1, pp. 153–160, 2024, doi: 10.21924/cst.9.1.2024.1419.

[84] D. Bedford and T. W. Sanchez, "Networks of Things," *Working Methods for Knowledge Management: Knowledge Networks*, pp. 257–273, 2021, doi: 10.1108/978-1-83982-948-220211016.

[85] M. Richards, *Software Architecture Pattern: Understanding Common Architecture Patterns and When to Use Them*. Boston: OReilly, 2015.

[86] C. Marche and M. Nitti, “Trust-Related Attacks and Their Detection: A Trust Management Model for the Social IoT,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3297–3308, 2021, doi: 10.1109/TNSM.2020.3046906.

[87] M. O. Ojo, S. Giordano, G. Procissi, and I. N. Seitanidis, “A Review of Low-End, Middle-End, and High-End Iot Devices,” *IEEE Access*, vol. 6, no. December, pp. 70528–70554, 2018, doi: 10.1109/ACCESS.2018.2879615.