DAFTAR PUSTAKA

Abdullah, D., Rahim, R., Utama Siahaan, A.P., Ulva, A.F., Fitri, Z., Malahayati, M. dan Harun, H., 2018, Super-Encryption Cryptography with IDEA and WAKE Algorithm, *Journal of Physics: Conference Series*, [Online] 1019 (1), tersedia di DOI:10.1088/1742-6596/1019/1/012039.

Ahn, W., Chung, M., Min, B.G. dan Seo, J., 2015, Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs, *International Journal of Distributed Sensor Networks*, [Online] 2015, tersedia di DOI:10.1155/2015/836258.

Altigani, A. dan Barry, B., 2013, A hybrid approach to secure transmitted messages using advanced encryption standard (AES) and Word Shift Coding Protocol, *Proceedings - 2013 International Conference on Computer, Electrical and Electronics Engineering: "Research Makes a Difference", ICCEEE 2013*, [Online] 134–139, tersedia di DOI:10.1109/ICCEEE.2013.6633920.

Amoah, R., 2016, *Formal Security Analysis of the DNP3-Secure Authentication Protocol*, [Online] (2016), 164, tersedia di *http://eprints.qut.edu.au/93798/1/Raphael_Amoah_Thesis.pdf*.

Amoah, R., Camtepe, S. dan Foo, E., 2016, Securing DNP3 Broadcast Communications in SCADA Systems, *IEEE Transactions on Industrial Informatics*, [Online] 12 (4), 1474–1485, tersedia di DOI:10.1109/TII.2016.2587883.

Atighehchi, K., Muntean, T., Parlanti, S., Rolland, R. dan Vallet, L., 2010, A Cryptographic Keys Transfer Protocol for Secure Communicating Systems, *2010 12th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, [Online], September 2010 IEEE., hal. 339–343, tersedia

di DOI:10.1109/SYNASC.2010.56.

Bartman, T. dan Carson, K., 2016, Securing communications for SCADA and critical industrial systems, *2016 69th Annual Conference for Protective Relay Engineers (CPRE)*, [Online], April 2016 IEEE., hal. 1–10, tersedia di DOI:10.1109/CPRE.2016.7914914.

Chen, B., Pattanaik, N., Goulart, A., Butler-Purry, K.L. dan Kundur, D., 2015, Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed, *Proceedings - CQR 2015: 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability*, [Online], 2015 hal. tersedia di DOI:10.1109/CQR.2015.7129084.

Clarke, G., Reynders, D. dan Wright, E., 2004, Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems, *Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems*, [Online] 1–537, tersedia di DOI:10.1016/B978-0-7506-5799-0.X5015-3.

Cremers, C., Dehnel-wild, M. dan Milner, K., 2017, Secure authentication in the grid: A formal analysis of DNP3: SAv5. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. [Online]. 10492 LNCS (June) hal.389–407. tersedia di DOI:10.1007/978-3-319-66402-6_23.

Cross, M., Hirota, M., Inoue, T., Kuchynska, A., Kuchynskyi, V., Macdonald, M., Michal, V., Negin, C., Pieraccini, M., Stubna, M. dan Yokoo, T., 2016, *Iaea Nuclear Energy Series Publications*, [Online] NG-T (3.4), 1–68, tersedia di *http://www.iaea.org/Publications/index.html*.

D'souza, F.J. dan Panchal, D., 2017, Advanced encryption standard (AES) security enhancement using hybrid approach, *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2017*, [Online] 2017-Janua647–652, tersedia di DOI:10.1109/CCAA.2017.8229881.

Darwish, I., Igbe, O., Celebi, O., Saadawi, T. dan Soryal, J., 2016, Smart Grid DNP3 Vulnerability Analysis and Experimentation, *Proceedings - 2nd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2015 - IEEE International Symposium of Smart Cloud, IEEE SSC 2015*, [Online] 141–147, tersedia di DOI:10.1109/CSCloud.2015.86.

Darwish, I., Igbe, O. dan Saadawi, T., 2015, Experimental and theoretical modeling of DNP3 attacks in smart grids, *2015 36th IEEE Sarnoff Symposium*, [Online] 155–160, tersedia di DOI:10.1109/SARNOF.2015.7324661.

Ding, H.J., Wang, Z.X., Wu, R.B. dan Zhao, Q.C., 2019, Enhancing the Security of Multi-agent Networked Control Systems Using QKD based Homomorphic Encryption, *Proceedings of the IEEE Conference on Decision and Control*, [Online] 2018-Decem (Cdc), 2080–2084, tersedia di DOI:10.1109/CDC.2018.8619432.

Dragomir, D., Gheorghe, L., Costea, S. dan Radovici, A., 2016, A Survey on Secure Communication Protocols for IoT Systems, *2016 International Workshop on Secure Internet of Things (SIoT)*, [Online], 2016 IEEE., hal. 47–62, tersedia di DOI:10.1109/SIoT.2016.012.

Drias, Z., Serhrouchni, A. dan Vogel, O., 2015a, Analysis of cyber security for industrial control systems, *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, [Online], Agustus 2015 IEEE., hal. 1–8, tersedia di DOI:10.1109/SSIC.2015.7245330.

Drias, Z., Serhrouchni, A. dan Vogel, O., 2015b, Taxonomy of attacks on industrial control protocols, *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*, [Online], Juli 2015 IEEE., hal. 1–6, tersedia di DOI:10.1109/NOTERE.2015.7293513.

East, S., Butts, J., Papa, M. dan Shenoi, S., 2009, A Taxonomy of Attacks on the DNP3 Protocol, *IFIP Advances in Information and Communication Technology*, [Online], hal. 67–81, tersedia di DOI:10.1007/978-3-642-04798-5_5.

Franco, D.J., Muhammed, A. Bin, Subramaniam, S.K., Abdullah, A., Silva, R.M. dan Akram, O.K., 2019, A Review on Current and Old SCADA Networks Applied to Water Distribution Systems, *2019 1st International Conference of Intelligent Computing and Engineering: Toward Intelligent Solutions for Developing and Empowering our Societies, ICOICE 2019*, [Online] tersedia di DOI:10.1109/ICOICE48418.2019.9035134.

Gilchrist, G., 2008, Secure authentication for DNP3, *IEEE Power and Energy Society 2008 General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, PES*, [Online], 2008 hal. tersedia di DOI:10.1109/PES.2008.4596147.

Hamdi, M., Rhouma, R. dan Belghith, S., 2017, A selective compression-encryption of images based on SPIHT coding and Chirikov Standard Map, *Signal Processing*, [Online] 131514–526, tersedia di DOI:10.1016/j.sigpro.2016.09.011.

Harba, E.S.I., 2017, Secure Data Encryption Through a Combination of AES, RSA and HMAC, *Engineering, Technology & Applied Science Research*, [Online] 7 (4), 1781–1785, tersedia di DOI:10.48084/etasr.1272.

Hong, N. dan Xuefeng, Z., 2013, A security framework for internet of things based on SM2 cipher algorithm, *Proceedings - 2013 International Conference on Computational and Information Sciences, ICCIS 2013*, [Online] 13–16, tersedia di DOI:10.1109/ICCIS.2013.12.

Hong, Z.Y., Qiu, Z.P., Zeng, S.L., Wang, S. De dan Sandrine, M., 2017, Research on fusion encryption algorithm for internet of things monitoring equipment,

Proceedings - 14th International Symposium on Pervasive Systems, Algorithms and Networks, I-SPAN 2017, 11th International Conference on Frontier of Computer Science and Technology, FCST 2017 and 3rd International Symposium of Creative Computing, ISCC 2017, [Online] 2017-Novem425–429, tersedia di DOI:10.1109/ISPAN-FCST-ISCC.2017.49.

Hou, A., Hu, C., Ma, K., Cai, Z., Huang, C. dan Pan, T., 2016, Research on modeling and simulation of communication in power SCADA system, *Proceedings of the 5th IEEE International Conference on Electric Utility Deregulation, Restructuring and Power Technologies, DRPT 2015*, [Online] 226–230, tersedia di DOI:10.1109/DRPT.2015.7432232.

IAEA, 2011, *Computer Security at Nuclear Facilities*, (no. 17),

IAEA, 2016, *Conducting Computer Security Assessments at Nuclear Facilities*, [Online]. tersedia di *http://www-pub.iaea.org/books/IAEABooks/10999/Conducting-Computer-Security-Assessments-at-Nuclear-Facilities%5Cnhttp://www-pub.iaea.org/MTCD/Publications/PDF/TDL006web.pdf*.

Isa, M.A.M., Ahmad, M.M., Sani, N.F.M., Hashim, H. dan Mahmod, R., 2014, Cryptographic key exchange protocol with message authentication codes (MAC) using finite state machine, *Procedia Computer Science*, [Online], 2014 Elsevier Masson SAS., hal. 263–270, tersedia di DOI:10.1016/j.procs.2014.11.061.

Islam, S.K.H., Amin, R., Biswas, G.P., Farash, M.S., Li, X. dan Kumari, S., 2017, An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments, *Journal of King Saud University - Computer and Information Sciences*, [Online] 29 (3), 311–324, tersedia di DOI:10.1016/j.jksuci.2015.08.002.

Jain, P. dan Tripathi, P., 2013, SCADA security: a review and enhancement for

DNP3 based systems, *CSI Transactions on ICT*, [Online] 1 (4), 301–308, tersedia di DOI:10.1007/s40012-013-0024-2.

Jolfaei, A. dan Mirghadri, A., 2010, Image Encryption Using Chaos and Block Cipher, *Computer and Information Science*, [Online] 4 (1), 172–185, tersedia di DOI:10.5539/cis.v4n1p172.

Kandasamy, N.K., 2020, An Investigation on Feasibility and Security for Cyberattacks on Generator Synchronization Process, *IEEE Transactions on Industrial Informatics*, [Online] 16 (9), 5825–5834, tersedia di DOI:10.1109/TII.2019.2957828.

Knapp, E., 2011, Standards and Regulations, *Industrial Network Security*, [Online], Elsevier., hal. 249–302, tersedia di DOI:10.1016/B978-1-59749-645-2.00010-0.

Krawec, W.O., 2016, Asymptotic analysis of a three state quantum cryptographic protocol, *2016 IEEE International Symposium on Information Theory (ISIT)*, [Online], Juli 2016 IEEE., hal. 2489–2493, tersedia di DOI:10.1109/ISIT.2016.7541747.

Mantere, M., Sailio, M. dan Noponen, S., 2013, Network Traffic Features for Anomaly Detection in Specific Industrial Control System Network, *Future Internet*, [Online] 5 (4), 460–473, tersedia di DOI:10.3390/fi5040460.

Michalski, J.T., Wyant, F.J., Duggan, D., Morris, A., Campbell, P., Clem, J., Parks, R., Martinez, L. dan Merza, M., 2010, *Secure Network Design Techniques for Safety System Applications at Nuclear Power Plants A Letter Report to the U . S . NRC*,

Mohamed, N.N., Mohd Yussof, Y., Saleh, M.A. dan Hashim, H., 2020, Hybrid Cryptographic Approach For Internet Of Things Applications: A Review, *Journal of Information and Communication Technology*, [Online] 19 (3), 279–319, tersedia di DOI:10.32890/jict2020.19.3.1.

Moreira, N., Molina, E., Lázaro, J., Jacob, E. dan Astarloa, A., 2016, Cyber-security in substation automation systems, *Renewable and Sustainable Energy Reviews*, [Online] 541552–1562, tersedia di DOI:10.1016/j.rser.2015.10.124.

Nivethan, J. dan Papa, M., 2016, A Linux-based firewall for the DNP3 protocol, *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, [Online], Mei 2016 IEEE., hal. 1–5, tersedia di DOI:10.1109/THS.2016.7568963.

Patel, S.C. dan Sanyal, P., 2008, Securing SCADA systems, *Information Management & Computer Security*, [Online] 16 (4), 398–414, tersedia di DOI:10.1108/09685220810908804.

Premnath, A.P., Jo, J.-Y. dan Kim, Y., 2014, Application of NTRU Cryptographic Algorithm for SCADA Security, *2014 11th International Conference on Information Technology: New Generations*, [Online], April 2014 IEEE., hal. 341–346, tersedia di DOI:10.1109/ITNG.2014.38.

Purevjav, S., Kim, T. dan Lee, H., 2016, Email encryption using hybrid cryptosystem based on Android, *International Conference on Advanced Communication Technology, ICACT*, [Online] 2016-March426–429, tersedia di DOI:10.1109/ICACT.2016.7423418.

Riyadi, E.H., Priyambodo, T.K. dan Putra, A.E., 2020, Real-time Testing on Improved Data Transmission Security in the Industrial Control System, *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, [Online], 10 Desember 2020 IEEE., hal. 129–134, tersedia di DOI:10.1109/ISRITI51436.2020.9315339.

Riyadi, E.H., Priyambodo, T.K. dan Putra, A.E., 2021, The Dynamic Symmetric Four-Key-Generators System for Securing Data Transmission in the Industrial Control System, *International Journal of Intelligent Engineering and Systems*, [Online] 14 (1), 376–386, tersedia di DOI:10.22266/ijies2021.0228.35.

Robinson, J.T., Saxton, T., Vojdani, A., Ambrose, D., Schimmel, G., Blaesing, R.R. dan Larson, R., 1995, Development of the Intercontrol Center Communications Protocol (ICCP) [power system control], *Proceedings of Power Industry Computer Applications Conference*, [Online] 449–455, tersedia di DOI:10.1109/PICA.1995.515277.

Saha, R., Geetha, G., Kumar, G., Kim, T.-H. dan Buchanan, W.J., 2019, MRC4: A Modified RC4 Algorithm Using Symmetric Random Function Generator for Improved Cryptographic Features, *IEEE Access*, [Online] 7172045–172054, tersedia di DOI:10.1109/ACCESS.2019.2956160.

Sari, R.N. dan Hayati, R.S., 2018, Beaufort Cipher Algorithm Analysis Based on the Power Lock-Blum Blum Shub in Securing Data, *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, [Online], Agustus 2018 IEEE., hal. 1–4, tersedia di DOI:10.1109/CITSM.2018.8674368.

Sembiring, I., 2017, Implementation of honeypot to detect and prevent distributed denial of service attack, *Proceedings - 2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering, ICITACEE 2016*, [Online] 345–350, tersedia di DOI:10.1109/ICITACEE.2016.7892469.

Setyaningsih, E., Wardoyo, R. dan Sari, A.K., 2020, Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution, *Digital Communications and Networks*, [Online] 6 (4), 486–503, tersedia di DOI:10.1016/j.dcan.2020.02.001.

Shabani, H. dan Ahmed, M., 2014, Novel IEEE 802. 15.4 protocol for modern SCADA communication systems, *2014 IEEE 8th International Power Engineering and Optimization Conference (PEOCO)*, [Online] (March), 597–601, tersedia di *http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6814498*.

Shahzad, A., Lee, M., Lee, C., Xiong, N., Kim, S., Lee, Y.-K.Y.K., Kim, K., Woo, S.-M.S. mi dan Jeong, G., 2016, The protocol design and New approach for SCADA security enhancement during sensors broadcasting system, *Multimedia Tools and Applications*, [Online] 75 (22), 14641–14668, tersedia di DOI:10.1007/s11042-015-3050-2.

Shahzad, A., Musa, S. dan Irfan, M., 2014a, N-Secure Cryptography Solution for SCADA Security Enhancement, *Trends in Applied Sciences Research*, [Online] tersedia di DOI:10.3923/tasr.2014.381.395.

Shahzad, A.A., Musa, S., Aborujilah, A. dan Irfan, M., 2014b, Secure cryptography testbed implementation for SCADA protocols security, *Proceedings - 2013 International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2013*, [Online], 2014 hal. tersedia di DOI:10.1109/ACSAT.2013.69.

Shahzad, Aa., Musa, S., Aborujilah, A. dan Irfan, M., 2014c, Industrial control systems (ICSs) vulnerabilities analysis and SCADA security enhancement using testbed encryption, *Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication - ICUIMC '14*, [Online], 2014 ACM Press, New York, New York, USA., hal. 1–6, tersedia di DOI:10.1145/2557977.2558061.

Shin, I., Eom, D. dan Song, B., 2015, The CoAP-based M2M gateway for distribution automation system using DNP3.0 in smart grid environment, *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, [Online], November 2015 IEEE., hal. 713–718, tersedia di DOI:10.1109/SmartGridComm.2015.7436385.

Shukla, A. dan Kumar, S., 2016, Analysis of secure watermarking based on DWT-SVD technique for piracy, *2016 International Conference on Computing, Communication and Automation (ICCCA)*, [Online], April 2016 IEEE., hal. 1110–1115, tersedia di DOI:10.1109/CCAA.2016.7813882.

Siddavatam, I.A.I.A. dan Kazi, F., 2016, Security assessment framework for cyber physical systems: A case-study of DNP3 protocol, *2015 IEEE Bombay Section Symposium: Frontiers of Technology: Fuelling Prosperity of Planet and People, IBSS 2015*, [Online] tersedia di DOI:10.1109/IBSS.2015.7456631.

Singh, C., Nivangune, A. dan Mrinal, P., 2016, *Function Code Based Vulnerability Analysis of DNP3*,

Singh, R., Panchbhaiya, I., Pandey, A. dan Goudar, R.H., 2015, Hybrid Encryption Scheme (HES): An approach for transmitting secure data over internet, *Procedia Computer Science*, [Online] 48 (C), 51–57, tersedia di DOI:10.1016/j.procs.2015.04.109.

Tare, B., Waghmare, S., Siddavatam, I., Kazi, F. dan Singh, N., 2016, Security analysis of DNP3 using CPN model with state space report representation using LDA, *2016 Indian Control Conference, ICC 2016 - Proceedings*, [Online] (Icc), 25–31, tersedia di DOI:10.1109/INDIANCC.2016.7441101.

Wang, J. dan Shi, D., 2018, Cyber-Attacks Related to Intelligent Electronic Devices and Their Countermeasures: A Review, *2018 53rd International Universities Power Engineering Conference (UPEC)*, [Online], September 2018 IEEE., hal. 1–6, tersedia di DOI:10.1109/UPEC.2018.8542059.

Wright, A.K., Kinast, J.A. dan McCarty, J., 2004, Low-Latency Cryptographic Protection for {SCADA} Communications, *Acns*, [Online] tersedia di DOI:10.1007/978-3-540-24852-1_19.

Xin, M., 2015, A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System, *Proceedings - 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2015*, [Online] 62–65, tersedia di DOI:10.1109/CyberC.2015.9.

Yu, P.H. dan Pooch, U.W., 2009, A secure dynamic cryptographic and encryption protocol for wireless networks, *IEEE EUROCON 2009*, [Online], Mei 2009

IEEE., hal. 1860–1865, tersedia di DOI:10.1109/EURCON.2009.5167898.

Zhang, J., Liu, H. dan Ni, L., 2020, A Secure Energy-Saving Communication and Encrypted Storage Model Based on RC4 for EHR, *IEEE Access*, [Online] 838995–39012, tersedia di DOI:10.1109/ACCESS.2020.2975208.