Pustaka

Ahamad, S.S. dan Pathan, A.S.K., 2019, Trusted service manager (TSM) based privacy preserving and secure mobile commerce framework with formal verification, *Complex Adaptive Systems Modeling*, [Online] 7 (1), 1–19, tersedia di DOI:10.1186/s40294-019-0064-z.

Akinyokun, N. dan Teague, V., 2017, Security and privacy implications of NFC-enabled contactless payment systems, *ACM International Conference Proceeding Series*, [Online] Part F1305, tersedia di DOI:10.1145/3098954.3103161.

Akter, S., Chakraborty, T., Khan, T.A., Chellappan, S. dan Islam, A.B.M.A. Al, 2017, Can You Get into the Middle of Near Field Communication?, *2017 IEEE 42nd Conference on Local Computer Networks (LCN)*, [Online] 365–373, tersedia di DOI:10.1109/LCN.2017.39.

Akter, S., Chellappan, S., Chakraborty, T., Khan, T.A., Rahman, A. dan Alim Al Islam, A.B.M., 2021, Man-in-the-Middle Attack on Contactless Payment over NFC Communications: Design, Implementation, Experiments and Detection, *IEEE Transactions on Dependable and Secure Computing*, [Online] 18 (6), 3012–3023, tersedia di DOI:10.1109/TDSC.2020.3030213.

Al-fayoumi, M. dan Nashwan, S., 2018, Performance Analysis of SAP-NFC Protocol, *International Journal of Communication Networks and Information Security (IJCNIS)*, 10 No 1 (April), 125,

Al-Haj, A. dan Al-Tameemi, M.A., 2018, Providing security for NFC-based payment systems using a management authentication server, *2018 4th International Conference on Information Management, ICIM 2018*, [Online] 184–187, tersedia di DOI:10.1109/INFOMAN.2018.8392832.

Al-Mamun, A., Rahman, S.S.M., Shaon, T.A. dan Hossain, M.A., 2017, Security analysis of AES and enhancing its security by modifying s-box with an additional byte, *International Journal of Computer Networks and Communications*, [Online] 9 (2), 69–88, tersedia di DOI:10.5121/ijcnc.2017.9206.

Alattar, M. dan Achemlal, M., 2014, Host-based card emulation: Development, security, and ecosystem impact analysis, *Proceedings - 16th IEEE International Conference on High Performance Computing and Communications, HPCC 2014, 11th IEEE International Conference on Embedded Software and Systems, ICESS 2014 and 6th International Symposium on Cyberspace Safety and Security*, [Online] 506–509, tersedia di DOI:10.1109/HPCC.2014.85.

Alliance, S.C., 2014, *A SMART CARD ALLIANCE MOBILE & NFC COUNCIL WHITE PAPER Host Card Emulation (HCE) 101*, [Online] (August), tersedia di *http://www.smartcardalliance.org/wp-content/uploads/HCE-101-WP-FINAL-081114-clean.pdf*.

Alzahrani, N., 2016, Securing Pharmaceutical and High-Value Products Against Tag Reapplication Attacks Using NFC Tags, *2016 IEEE International*

Conference on Smart Computing (SMARTCOMP), [Online] tersedia di DOI:10.1109/SMARTCOMP.2016.7501715.

Aminudin, A. dan Budi Cahyono, E., 2021, A Practical Analysis of the Fermat Factorization and Pollard Rho Method for Factoring Integers, *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, [Online] 12 (1), 33, tersedia di DOI:10.24843/lkjiti.2021.v12.i01.p04.

Anonim, 2018, ISO / IEC 7816 Part 4 : Interindustry command for interchange, [Online] tersedia di *https://www.iso.org/obp*.

Asaduzzaman, A., Mazumder, S. dan Salinas, S., 2017, A Security-Aware Near Field Communication Architecture, *2017 International Conference on Networking, Systems and Security (NSysS)*, (January),

Badra, M. dan Badra, R.B., 2016, A Lightweight Security Protocol for NFC-based Mobile Payments, *Procedia Computer Science*, [Online] 83 (Ant), 705–711, tersedia di DOI:10.1016/j.procs.2016.04.156.

Bahig, H.M., Mahdi, M.A., Alutaibi, K.A., AlGhadhban, A. dan Bahig, H.M., 2020, Performance Analysis of Fermat Factorization Algorithms, *International Journal of Advanced Computer Science and Applications*, [Online] 11 (12), 340–352, tersedia di DOI:10.14569/IJACSA.2020.0111242.

Cavdar, D. dan Tomur, E., 2015, A practical NFC relay attack on mobile devices using card emulation mode, *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2015 - Proceedings*, [Online] (May), 1308–1312, tersedia di DOI:10.1109/MIPRO.2015.7160477.

Chattha, N.A., 2014, NFC - Vulnerabilities and Defense, *2014 Conference on Information Assurance and Cyber Security (CIACS) NFC*, (1), 35–38,

Chen, C.H., Lin, I.C. dan Yang, C.C., 2014, NFC attacks analysis and survey, *Proceedings - 2014 8th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2014*, [Online] 458–462, tersedia di DOI:10.1109/IMIS.2014.66.

Coskun, V., Ozdenizci, B. dan Ok, K., 2013, A survey on near field communication (NFC) technology, *Wireless Personal Communications*, [Online] 71 (3), 2259–2294, tersedia di DOI:10.1007/s11277-012-0935-5.

Coskun, V., Ozdenizci, B. dan Ok, K., 2015, The Survey on Near Field Communication., *Sensors (Basel, Switzerland)*, [Online] 15 (6), 13348–13405, tersedia di DOI:10.3390/s150613348.

Crossman, M.A. dan Liu, H., 2016, Two-factor authentication through near field communication, *2016 IEEE Symposium on Technologies for Homeland Security, HST 2016*, [Online] tersedia di DOI:10.1109/THS.2016.7568941.

Dang, F., Zhai, E., Li, Z., Zhou, P., Mohaisen, A., Bian, K., Wen, Q. dan Li, M., 2019, Pricing Data Tampering in Automated Fare Collection with NFC-Equipped Smartphones, *IEEE Transactions on Mobile Computing*, [Online] 18 (5), 1159–1173, tersedia di DOI:10.1109/TMC.2018.2853114.

Dang, F., Zhou, P., Li, Z. dan Liu, Y., 2017a, NFC-enabled attack on cyber physical systems: A practical case study, *2017 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2017*, [Online] 289–294, tersedia di DOI:10.1109/INFCOMW.2017.8116391.

Dang, F., Zhou, P., Li, Z., Zhai, E., Mohaisen, A., Wen, Q. dan Li, M., 2017b,

Large-scale invisible attack on AFC systems with NFC-equipped smartphones, *Proceedings - IEEE INFOCOM*, [Online] tersedia di DOI:10.1109/INFOCOM.2017.8057219.

Fahrianto, F., Lubis, M.F. dan Fiade, A., 2016, Denial-of-Service attack Possibilities on NFC Technology, *2016 4th International Conference on Cyber and IT Service Management*, [Online] (April), tersedia di DOI:10.1109/CITSM.2016.7577582.

Fan, K., Song, P. dan Yang, Y., 2017, ULMAP : Ultralightweight NFC Mutual Authentication Protocol with Pseudonyms in the Tag for IoT in 5G, *Mobile Information Systems*, 2017 (April),

Grønli, T.M., Pourghomi, P. dan Ghinea, G., 2015, Towards NFC payments using a lightweight architecture for the Web of Things, *Computing*, [Online] 97 (10), 985–999, tersedia di DOI:10.1007/s00607-014-0397-6.

Htet, M., 2020, *EXTENDED POLLARD ' S RHO FACTORIZATION ALGORITHM FOR FINDING EXTENDED POLLARD ' S RHO FACTORIZATION ALGORITHM FOR*, [Online] (October), tersedia di DOI:10.13140/RG.2.2.34889.16485.

Jignesh, P., 2013, NEAR FIELD COMMUNICATION - THE FUTURE TECHNOLOGY FOR AN INTERACTIVE WORLD, *International Journal of Engineering Research and Science & Technology*, 2. No. 2 (May 2013),

Kodama, Y., Odajima, T., Arima, E. dan Sato, M., 2020, Evaluation of Power Management Control on the Supercomputer Fugaku, *Proceedings - IEEE International Conference on Cluster Computing, ICCC*, [Online] 2020-Septe484–493, tersedia di DOI:10.1109/CLUSTER49012.2020.00069.

Luo, J.N. dan Yang, M.H., 2019, EMV-compatible offline mobile payment protocol with mutual authentication, *Sensors (Switzerland)*, [Online] 19 (21), 1–24, tersedia di DOI:10.3390/s19214611.

Luo, J.N., Yang, M.H. dan Huang, S.Y., 2016, An Unlinkable Anonymous Payment Scheme based on near field communication, *Computers and Electrical Engineering*, [Online] 49198–206, tersedia di DOI:10.1016/j.compeleceng.2015.08.007.

Macias, E., Jacobi, R. dan Wyatt, J., 2014, NFC Card Emulation Using the TRF7970A, *SLOA208*, (November), 1–35,

Macias, E. dan Wyatt, J., 2016, NFC Active and Passive Peer-to-Peer Communication Using the TRF7970A, *SLOA192A*, (April), 1–34,

Madhoun, N. El, Bertin, E. dan Pujolle, G., 2018, An overview of the EMV protocol and its security vulnerabilities, *2018 4th International Conference on Mobile and Secure Services, MOBISECSERV 2018*, [Online] 2018-Febru (February), 1–5, tersedia di DOI:10.1109/MOBISECSERV.2018.8311444.

El Madhoun, N., Bertin, E. dan Pujolle, G., 2018, For Small Merchants: A Secure Smartphone-Based Architecture to Process and Accept NFC Payments, *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, [Online] 403–411, tersedia di DOI:10.1109/TrustCom/BigDataSE.2018.00067.

Madhoun, N. El, Bertin, E. dan Pujolle, G., 2019, The EMV Payment System: Is It

Reliable?, *2019 3rd Cyber Security in Networking Conference, CSNet 2019*, [Online] (2), 80–85, tersedia di DOI:10.1109/CSNet47905.2019.9108846.

Mahansaria, D. dan Roy, U.K., 2019, Secure authentication for ATM transactions using NFC technology, *Proceedings - International Carnahan Conference on Security Technology*, [Online] 2019-Octob1–5, tersedia di DOI:10.1109/CCST.2019.8888427.

Main, J., 2009, *NFC Technology Overview*, (September),

Minihold, R., 2011, Near Field Communication (NFC) Technology and Measurements, *White Paper*, 26,

Munch-Ellingsen, A., Karlsen, R., Andersen, A. dan Akselsen, S., 2015, Two-factor authentication for android host card emulated contactless cards, *2015 1st Conference on Mobile and Secure Services, MOBISECSERV 2015*, [Online] tersedia di DOI:10.1109/MOBISECSERV.2015.7072874.

Nashwan, S., 2017, Secure Authentication Protocol for Mobile Payment, *International Journal of Computer Science and Network Security*, [Online] 17 (8), 256–263, tersedia di DOI:10.26599/tst.2018.9010031.

NFC Forum, 2012, NFC Controller Interface (NCI) Specification Technical Specification NFC Forum TM, *NFC Forum, Inc*,

NFC Forum, 2006, *NFC Data Exchange Format (NDEF) 1.0*, 1–25,

Oad, K., 2021, *Reduce the Complexity of Big Number Factoring for RSA Breaking Reduce the Complexity of Big Number Factoring for RSA Breaking By Kanwal Oad Submitted in partial fulfillment of the requirements for the thesis , Master of Applied Computer Science in the " H*, (October),

Ondrus, J. dan Pigneur, Y., 2009, Near field communication: An assessment for future payment systems, *Information Systems and e-Business Management*, [Online] 7 (3), 347–361, tersedia di DOI:10.1007/s10257-008-0093-1.

Özcanhan, M.H., Dalkiliç, G. dan Utku, S., 2014, Cryptographically supported NFC tags in medication for better inpatient safety patient facing systems, *Journal of Medical Systems*, [Online] 38 (8), tersedia di DOI:10.1007/s10916-014-0061-x.

Pannifer, S., Clark, D. dan Birch, D., 2014, *HCE and SIM secure element : It's not black and white*, 1–12,

Park, J., Lee, S., Bouk, S.H. dan Kim, D., 2015, *6LoWPAN Adaptation Protocol for IPv6 Packet Transmission Over NFC Device*, 541–543,

Pourghomi, P., Abi-char, P.E. dan Ghinea, G., 2015, Towards a mobile payment market: A Comparative Analysis of Host Card Emulation and Secure Element, *International Journal of Computer Science and Information Security (IJCSIS)*, 13 (12), 156–164,

Pourghomi, P., Saeed, M.Q. dan Ghinea, G., 2013, A Proposed NFC Payment Application, *International Journal of Advanced Computer Science and Applications*, [Online] 4. No. 8 (December), 173–181, tersedia di DOI:10.14569/IJACSA.2013.040824.

Pourghomi, P., Seker, S.E., Ghinea, G. dan Masri, W., 2016, Java Implementation of a Cloud-based SIM Secure Element NFC Payment Protocol, *International Journal of Security and Its Applications*, [Online] 10 (12), 261–282, tersedia di DOI:10.14257/ijsia.2016.10.12.21.

Roland, M. dan Langer, J., 2012, Practical Attack Scenarios on Secure Element-

enabled Mobile Devices, *Fourth International Workshop on Near Field Communication*, [Online] tersedia di DOI:10.1109/NFC.2012.10.

Rukhin, A., Soto, J. dan Nechvatal, J., 2010, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, *Nist Special Publication*, [Online] 22 (April), 1/1--G/1, tersedia di *http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf*.

Sethia, D., Gupta, D. dan Saran, H., 2018, NFC Secure Element-Based Mutual Authentication and Attestation for IoT Access, *IEEE Transactions on Consumer Electronics*, [Online] 64 (4), 470–479, tersedia di DOI:10.1109/TCE.2018.2873181.

Skibba, R., 2021, Japan's Fugaku Supercomputer Crushes Competition, But Likely Not for Long, *Engineering*, [Online] 7 (1), 6–7, tersedia di DOI:10.1016/j.eng.2020.12.003.

Somsuk, K., 2020, The new integer factorization algorithm based on Fermat's Factorization Algorithm and Euler's theorem, *International Journal of Electrical and Computer Engineering*, [Online] 10 (2), 1469–1476, tersedia di DOI:10.11591/ijece.v10i2.pp1469-1476.

Stallings, W., 2014, *Cryptography and Network Security: Principles and Practice, International Edition: Principles and Practice*, [Online]. tersedia di *https://books.google.com/books?id=q_6pBwAAQBAJ&pgis=1*.

Sujithra, M., Padmavathi, G. dan Narayanan, S., 2015, Mobile device data security: A cryptographic approach by outsourcing mobile data to cloud, *Procedia Computer Science*, [Online] 47 (C), 480–485, tersedia di DOI:10.1016/j.procs.2015.03.232.

Suparta, W., 2012, Application of near field communication technology for mobile airline ticketing, *Journal of Computer Science*, [Online] 8 (8), 1235–1243, tersedia di DOI:10.3844/jcssp.2012.1235.1243.

Urien, P. dan Piramuthu, S., 2013, *Framework and Authentication Protocols for Smartphone , NFC , and RFID in Retail Transactions*, 77–82,

Wenxing, O., Lei, W., Yu, Z. dan Changhong, Y., 2015, Research on Anti-eavesdropping Communication Mechanism for NFC, *Proceedings - 2015 7th International Conference on Measuring Technology and Mechatronics Automation, ICMTMA 2015*, [Online] 839–841, tersedia di DOI:10.1109/ICMTMA.2015.206.