normal and malicious apps. It was confirmed that the accuracy was improved by about 2% by including meaningful feature data such as the frequency of the top 20 permissions based on the importance of feature information using the frequency of use of the permission. Since it is important to minimize misdetection and misdetection and make accurate judgments in detecting normal and malicious apps, an ML model optimized for classification has been implemented. In this study, as the number of malicious apps that develop day-by-day increases, it was judged that it is important to detect malicious apps through the ML model accurately. However, simply using permission as a criterion for distinguishing between normal and malicious apps is not enough to detect all malicious apps appearing with new attack technology. In addition, it is expected that higher accuracy of the detection model can be expected by combining feature information effective in detecting malicious apps, such as APIs that access and control sensitive data from users or adding other detection criteria. In future research, recent attackers bypass malicious app detection using obfuscation that hides malicious code and prevents static analysis of malicious apps. It is necessary to think about how to detect malicious apps with such obfuscation.

REFERENCES

[1] J. A. Odey, B. Ola, and I. Agbonlahor, "The Cyber Crime of Juice Jacking in Developing Economies: Susceptibilities, Consequences and Control Measures," *European Journal of Information Technologies and Computer Science*, vol. 1, no. 5, pp. 1-5, 2021.

[2] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, and S. Venkatraman, "Robust intelligent malware detection using deep learning," *IEEE Access*, vol. 7, pp. 46717-46738, 2019.

[3] Joon-ho Han, "Mobile Hacking Malicious Apps Surge," Oct. 7, 2020. [Online]. Available: https://www.hanjunho.com/35/?q=YToxOntzOjEyOiJrZXl3b3JkX3R5cGUiO3M6MzoiYWxsIjt9&bmode=view&idx=5050914&t=board.

[4] EST security, "Play Store identified as main distribution vector for most Android malware," Nov. 12, 2020. [Online]. Available: https://blo g.alyac.co.kr/3370.

[5] Y. J. Lee, "Voice phishing gang arrested for extorting $264 million by inducing malicious app installation," May. 31, 2021. [Online]. Available: https://www.news1.kr/articles/?4323269.

[6] S. E. Kang, H. S. Yoon, and S. H. Jung, "Design and Implementation of API Extraction Method for Android Malicious Code Analysis Using Xposed," *Journal of the Korea Institute of Information Security & Cryptology*, vol. 29, no. 1, pp. 105-115, Feb. 2019.

[7] G. Y. Kim, S. R. Kim, Y. J. Jeon, and J. S. Kim, "A Trend of Machine Learning for Android Malware Detection and Permission Based Android Malware Detection using Deep Learning," *Korean Society of Digital Forensics*, vol. 14, no. 3, pp. 316-326, Sep. 2020.

[8] A. Afianian, S. Niksefat, B. Sadeghiyan, and D. Baptiste, "Malware dynamic analysis evasion techniques: A survey," *ACM Computing Surveys (CSUR)*, vol. 52, no. 6, pp. 1-28, 2019.

[9] Z. Fang, J. Wang, J. Geng, and X. Kan, "Feature selection for malware detection based on reinforcement learning," *IEEE Access*, vol. 7, pp. 176177-176187, 2019.

[10] J. G. Joo, I. S. Jeong, and S. H. Kang, "An Optimal Feature Selection Method to Detect Malwares in Real Time Using Machine Learning," *Journal of Korea, Multimedia Society*, vol. 22, no. 2, pp. 203-209, Feb. 2019.

[11] Y. Chang, B. Liu, L. Cong, H. Deng, J. Li, and Y. Chen, "Vulnerability Parser: A Static Vulnerability Analysis System for Android Applications," *Journal of Physics: Conference Series*, vol. 1288, no. 1, Aug. 2019.

[12] H. W. Lee and H. S. Lee, "Optimal Machine Learning Model for Detecting Normal and Malicious Android Apps," *The Journal of the Internet of Things in Korea*, vol. 6, no. 2, pp. 1-10, Jun. 2020.

[13] M. J. Kim and J. C. Ryou, "Development of LLDB module for potential vulnerability analysis in iOS Application," *Journal of Internet Computing and Services*, vol. 20, no. 4, pp. 13-19, 2019.

[14] K. W. Lee, S. T. Oh, and Y. Yoon, "Modeling and Selecting Optimal Features for Machine Learning Based Detections of Android Malwares," *Thesis Collection of the Korean Society for Information Processing*, vol. 8, no. 11, pp. 427-432, Nov. 2019.

[15] V. Sihag, M. Vardhan, P. Singh, G. Choudhary, and S. Son, "De-lady: Deep learning based android malware detection using dynamic features," *Journal of Internet Services and Information Security (JISIS)*, vol. 11, no. 2, pp. 34-45, 2021.

[16] H. W. Lee and H. S. Lee, "Optimal Machine Learning Model for Detecting Normal and Malicious Android Apps," *Journal of The Korea Internet of Things Society*, vol. 6, no. 2, pp. 1-10, 2020.

[17] J. Park, T. Kim, Y. Shin, J. Kim, and E. Choi, "Design and Implementation of a Pre-processing Method for Image-based Deep Learning of Malware," *Journal of Korea Multimedia Society*, vol. 23, no. 5, pp. 650-657, 2020.

[18] Android Developer, "Manifest.Permission," [Online]. Available: https://developer.android.com/reference/android/Manifest.permission

[19] S. I. Imtiaz, S. ur Rehman, A. R. Javed, Z. Jalil, X. Liu, and W. S. Alnumay, "DeepAMD: Detection and identification of Android malware using high-efficient Deep Artificial Neural Network," *Future Generation computer systems*, vol. 115, pp. 844-856, 2021.

[20] B. H. Kim and M. T. Kwon, "Measures for Adware and Spyware," *Journal of Convergence Security*, vo1. 6, no. 4, pp. 41-47, Dec. 2006.

[21] G. B. Lee, J. Y. Ok, and E. G. Lim, "Method of Signature Extraction and Selection for Ransomware Dynamic Analysis," *KIISE Transactions on Computing Practices (KTCP)*, vol. 24, no. 2, pp. 99-104, Feb. 2018.

[22] D. Maimon and E. R. Louderback, "Cyber-dependent crimes: An interdisciplinary review," *Annual Review of Criminology*, vol. 2, pp. 191-216, 2019.

[23] Korea Internet & Security Agency (KISA) Internet Protect World & KrCERT, "What is Smishing?," [Online]. Available: https://www.boho.or.kr/cyber/smishing.do.

[24] S. M. Choi, "Cyber threats analysis using machine learning," M.S. thesis, Dept. CSE. Kor., Han-yang Univ., Seoul, Korea, 2020.

[25] Y. Kim and S. Chang, "A Hybrid Approach of Using Both Simulation plus Neural Networks for Window Design Optimization and HVAC Energy Consumption Prediction Modeling," *International Journal of Structural and Civil Engineering Research*, vol. 8, no. 4, pp. 300-309, Nov. 2019.

[26] B. Park, I. Yoo, J. Lee, S. Jang, S. Y. Kim, and Y. Kim, "A Reference Frame Selection Method Using RGB Vector and Object Feature Information of Immersive 360° Media," *Journal of IKEEE*, vol. 24, no. 4, pp. 1050-1057, 2020.

[27] J. M. Koo, S. D. Na, J. H. Cho, and M. N. Kim, "Melanoma Classification Algorithm using Gray-level Conversion Matrix Feature and Support Vector Machine," *Journal of Korea Multimedia Society*, vol. 21, no. 2, pp. 130-137, 2018.

[28] Y. H. Jo, "Early ransomware detection using machine learning," M.S. thesis, Dept. CSE. Kor., Kook-Min Univ., Seoul, Korea, 2020.

[29] G. U. Park and I. Jung, "Comparison of resampling methods for dealing with imbalanced data in binary classification problem," *The Korean Journal of Applied Statistics*, vol. 32, no. 3, pp. 349-374, 2019.

[30] Y. Lei, B. Yang, X. Jiang, F. Jia, N. Li, and A. K. Nandi, "Applications of machine learning to machine fault diagnosis: A review and roadmap," *Mechanical Systems and Signal Processing*, vol. 138, pp. 1-39, 2020.

[31] A. Arora, S. K. Peddoju, and M. Conti, "Permpair: Android malware detection using permission pairs," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1968-1982, 2019.

[32] J. M. Jung, H. J. Kim, S. J. Cho, S. C. Han, and K. W. Suh, "Efficient Android Malware Detection Using API Rank and Machine Learning," *Journal of Internet Services and Information Security*, vol. 9, no. 1, pp. 48-59. Feb. 2019.

[33] S. H. Park, M. Y. Kang, J. H. Park, S. J. Cho, and S. C. Han, "Analyzing the Effects of API Calls in Android Malware Detection Using Machine Learning," *Journal of Korea Institute of Information Security & Cryptology*, vol. 48, no. 3, pp. 257-263, Mar. 2021.

[34] Z. Ma, H. Ge, Y. Liu, M. Zhao, and J. Ma, "A combination method for android malware detection based on control flow graphs and machine learning algorithms," *IEEE access*, vol. 7, pp. 21235-21245, 2019.

[35] S. I. Imtiaz, S. U. Rehman, A. R. Javed, Z Jalil, X. Liu, and W. S. Alnumay, "Deep AMD: Detection and identification of Android malware using high-efficient Deep Artificial Neural Network," *Future Generation Computer Systems*, vo1. 115, pp. 844–856, Feb. 2021.