## REFERENCES


Abdullayev, V., & Chauhan, A. S. (2023). SQL Injection Attack: Quick View. *MJCS*. https://doi.org/10.58496/mjcs/2023/006

Abikoye, O. C., Abubakar, A., Dokoro, A. H., Oluwatobi, A. N., & Kayode, A. A. (2020). A Novel Technique to Prevent SQL Injection and Cross-Site Scripting Attacks Using Knuth-Morris-Pratt String Match Algorithm. *Eurasip Journal on Information Security*. https://doi.org/10.1186/s13635-020-00113-y

Aboughadareh, S., Csallner, C., & Azarmi, M. (2014). *Mixed-Mode Malware and Its Analysis*. https://doi.org/10.1145/2689702.2689703

Agrawal, D., Baktır, S., Karakoyunlu, D., Rohatgi, P., & Sunar, B. (2007). *Trojan Detection Using IC Fingerprinting*. https://doi.org/10.1109/sp.2007.36

Alazab, M., Venkataraman, S., & Watters, P. A. (2010). *Towards Understanding Malware Behaviour by the Extraction of API Calls*. https://doi.org/10.1109/ctc.2010.8

Alhashmi, A. A., Ghaleb, F. A., Al-Marghilani, A., Yahya, A. E., Ebad, S. A., Saqib, M. S. M., & Darem, A. B. (2022). Deep-Ensemble and Multifaceted Behavioural Malware Variant Detection Model. *Ieee Access*. https://doi.org/10.1109/access.2022.3168794

Alkabani, Y., & Koushanfar, F. (2009). *Consistency-Based Characterization for IC Trojan Detection*. https://doi.org/10.1145/1687399.1687426

Alsattam, F., Al-Akhras, M., Almasri, M., & Alawairdhi, M. (2020). Rule-Based Approach to Detect IoT Malicious Files. *Journal of Computer Science*. https://doi.org/10.3844/jcssp.2020.1203.1211

Aras, A. O. (2023). *A Short Survey on Malware Behavioural Features Collection From AgTech Environments*. https://doi.org/10.36227/techrxiv.22548892.v1

Arfaj, B. A. B., Mishra, S., & Alshehri, M. (2022). Efficacy of Unconventional Penetration Testing Practices. *Intelligent Automation & Soft Computing*. https://doi.org/10.32604/iasc.2022.019485

Aslan, O., Ozkan-Okay, M., & Gupta, D. (2021). A Review of Cloud-Based Malware Detection System: Opportunities, Advances and Challenges. *European Journal of Engineering and Technology Research*. https://doi.org/10.24018/ejeng.2021.6.3.2372

*Automatic Analysis of Malware Behaviour With SVM*. (2016). https://doi.org/10.18178/wcse.2016.06.019

Aydogan, E., & Sen, S. (2015). *Automatic Generation of Mobile Malwares Using Genetic Programming*. https://doi.org/10.1007/978-3-319-16549-3_60

Azizi, A., Tahmid, I. A., Waheed, A., Mangaokar, N., Pu, J., Javed, M., Reddy, C. K., & Viswanath, B. (2021). *T-Miner: A Generative Approach to Defend Against Trojan Attacks on DNN-based Text Classification*. https://doi.org/10.48550/arxiv.2103.04264

Baysa, D., Low, R. M., & Stamp, M. (2013). Structural Entropy and Metamorphic Malware. *Journal of Computer Virology and Hacking Techniques*. https://doi.org/10.1007/s11416-013-0185-4

Benard, M. C., Charles, M., Charo, J. S., & Mgala, M. (2021). Cyber-Crimes Issues on Social Media Usage Among Higher Learning Institutions Students in Dar ES Salaam Region, Tanzania. *International Journal of*

*Scientific Research in Science Engineering and Technology*. https://doi.org/10.32628/ijsrset218418

Biondi, F., Déchelle, F., & Legay, A. (2017). *MASSE: Modular Automated Syntactic Signature Extraction*. https://doi.org/10.1109/issrew.2017.74

Black, P., Gondal, I., Bagirov, A. M., & Moniruzzaman. (2021). Malware Variant Identification Using Incremental Clustering. *Electronics*. https://doi.org/10.3390/electronics10141628

Cahyanto, K. A., Al Hilmi, M. A., & Mustamiin, M. Z. (2022). Pengujian Rule-Based Pada Dataset Log Server Menggunakan Support Vector Machine Berbasis Linear Discriminat Analysis Untuk Deteksi Malicious Activity. *Jurnal Teknologi Informasi Dan Ilmu Komputer*. https://doi.org/10.25126/jtiik.2022924107

Carapella, M., Vecchio, A. D., Nardi, L., Pirozzi, A., & Visaggio, C. A. (2020). *About the Robustness and Looseness of Yara Rules*. https://doi.org/10.1007/978-3-030-64881-7_7

Chaganti, R., Sowmya, V., Alazab, M., & Pham, T. D. (2021). *Stegomalware: A Systematic Survey of MalwareHiding and Detection in Images, Machine LearningModels and Research Challenges*. https://doi.org/10.48550/arxiv.2110.02504

Chakraborty, R. S., Wolff, F., Sauseng, P., Papachristou, C., & Bhunia, S. (2009). *MERO: A Statistical Approach for Hardware Trojan Detection*. https://doi.org/10.1007/978-3-642-04138-9_28

Chen, Z., Wei, P., & Delis, A. (2007). Catching Remote Administration Trojans (<i>RATs</I>). *Software Practice and Experience*. https://doi.org/10.1002/spe.837

Cheng, S., Tao, G., Liu, Y., An, S., Xu, X., Feng, S., Shen, G., Zhang, K., Xu, Q., Ma, S., & Zhang, X. (2023). *BEAGLE: Forensics of Deep Learning Backdoor Attack for Better Defense*. https://doi.org/10.14722/ndss.2023.24944

Dakov, S., & Malinova, A. (2021). A Survey of E-Commerce Security Threats and Solutions. *Proceedings of Cbu in Natural Sciences and Ict*. https://doi.org/10.12955/pns.v2.135

Dalai, A. K., & Jena, S. K. (2017). Neutralizing SQL Injection Attack Using Server Side Code Modification in Web Applications. *Security and Communication Networks*. https://doi.org/10.1155/2017/3825373

Darem, A. B., Ghaleb, F. A., Alhashmi, A. A., Abawajy, J., Alanazi, S. M., & Al-Rezami, A. Y. (2021). An Adaptive Behavioural-Based Incremental Batch Learning Malware Variants Detection Model Using Concept Drift Detection and Sequential Deep Learning. *Ieee Access*. https://doi.org/10.1109/access.2021.3093366

Dawadi, B. R., Adhikari, B., & Srivastava, D. K. (2023). Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks. *Sensors*. https://doi.org/10.3390/s23042073

dmi. (n.d.). *Menkominfo Respons Jutaan Web Judi Online Nebeng Situs Pemerintah*. teknologi. Retrieved February 20, 2024, from https://www.cnnindonesia.com/teknologi/20230823195209-192-

989695/menkominfo-respons-jutaan-web-judi-online-nebeng-situs-pemerintah

Efe, A., & Hussin, S. H. S. (2020). Malware Visualization Techniques. *International Journal of Applied Mathematics Electronics and Computers*. https://doi.org/10.18100/ijamec.526813

Fujii, S., Yamagishi, R., & Yamauchi, T. (2022). Survey and Analysis on ATT&CK Mapping Function of Online Sandbox for Understanding and Efficient Using. *Journal of Information Processing*. https://doi.org/10.2197/ipsjjip.30.807

Ghanem, M. C., & Chen, T. (2019). Reinforcement Learning for Efficient Network Penetration Testing. *Information*. https://doi.org/10.3390/info11010006

Han, S., Lee, K., & Lee, S.-J. (2009). *Packed PE File Detection for Malware Forensics*. https://doi.org/10.1109/csa.2009.5404211

Hashemi, S., Keshavarz-Haddad, A., & Haeri, M. A. (2017). An Entropy-Based Distance Measure for Analyzing and Detecting Metamorphic Malware. *Applied Intelligence*. https://doi.org/10.1007/s10489-017-1045-6

Hassan, M. H., Ahmad, B., Esha, A., Risha, R., & Hasan, M. S. (2022). Important Factors to Remember When Constructing a Cross-Site Scripting Prevention Mechanism. *Bulletin of Electrical Engineering and Informatics*. https://doi.org/10.11591/eei.v11i2.3557

He, Y., Zamani, E. D., Ni, K., Yevseyeva, I., & Luo, C. (2023). Artificial Intelligence–Based Ethical Hacking for Health Information Systems:

Simulation Study. *Journal of Medical Internet Research*. https://doi.org/10.2196/41748

Hernawan, F. Y., Hidayatulloh, I., & Adam, I. F. (2021). Hybrid Method Integrating SQL-IF and Naïve Bayes for SQL Injection Attack Avoidance. *Journal of Engineering and Applied Technology*. https://doi.org/10.21831/jeatech.v1i2.35497

Husin, H. S., Cui, L., Husny Hamid, H. R., & Abdullah, N. Y. (2013). *Time Series Analysis of Web Server Logs for an Online Newspaper*. https://doi.org/10.1145/2448556.2448557

Ikebe, M., & Yoshida, K. (2013). *An Integrated Distributed Log Management System With Metadata for Network Operation*. https://doi.org/10.1109/cisis.2013.134

Jeon, J., Park, J. H., & Jeong, Y.-S. (2020). Dynamic Analysis for IoT Malware Detection With Convolution Neural Network Model. *Ieee Access*. https://doi.org/10.1109/access.2020.2995887

Jin, J., & Lin, X. (2022). Web Log Analysis and Security Assessment Method Based on Data Mining. *Computational Intelligence and Neuroscience*. https://doi.org/10.1155/2022/8485014

Kareem, F. Q., Ameen, S. Y., Salih, A. A., Ahmed, D. M., Kak, S. F., Yasin, H. M., Ibrahim, I. M., Ahmed, A. M., Rashid, Z. N., & Omar, N. (2021). SQL Injection Attacks Prevention System Technology: Review. *Asian Journal of Research in Computer Science*. https://doi.org/10.9734/ajrcos/2021/v10i330242

Karunakaran, S., Arun, N., kumar, M. A., & Aswiin, S. S. (2022). Cryptography Based Secured Internet Banking Using Multifactor Authentication. *JCSCS*. https://doi.org/10.46610/jcscs.2022.v01i02.001

Kharod, S., Sharma, N., & Sharma, A. (2015). *An Improved Hashing Based Password Security Scheme Using Salting and Differential Masking*. https://doi.org/10.1109/icrito.2015.7359225

Kolouri, S., Saha, A., Pirsiavash, H., & Hoffmann, H. (2020). *Universal Litmus Patterns: Revealing Backdoor Attacks in CNNs*. https://doi.org/10.1109/cvpr42600.2020.00038

KOMINFO, P. (n.d.). *Siaran Pers No. 01/HM/KOMINFO/01/2024 tentang Putus Akses Lebih dari 800 Ribu Konten, Gerak Cepat Menteri Budi Arie Berantas Judi Online*. Website Resmi Kementerian Komunikasi dan Informatika RI. Retrieved February 20, 2024, from http:///index.php/content/detail/53893/siaran-pers-no-01hmkominfo012024-tentang-putus-akses-lebih-dari-800-ribu-konten-gerak-cepat-menteri-budi-arie-berantas-judi-online/0/siaran_pers

Krishna, T. S. R. (2021). Malware Detection Using Deep Learning. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2021.35426

Lin, X., Lei, L., Wang, Y., Jing, J., Sun, K., & Zhou, Q. (2018). *A Measurement Study on Linux Container Security*. https://doi.org/10.1145/3274694.3274720

Liu, L., He, X., Liu, L., Qing, L., Fang, Y., & Liu, J. (2019). Capturing the Symptoms of Malicious Code in Electronic Documents by File's Entropy

Signal Combined With Machine Learning. *Applied Soft Computing*. https://doi.org/10.1016/j.asoc.2019.105598

Lorenzini, G., Shaw, D., & Elger, B. S. (2022). It Takes a Pirate to Know One: Ethical Hackers for Healthcare Cybersecurity. *BMC Medical Ethics*. https://doi.org/10.1186/s12910-022-00872-y

Lyda, R., & Hamrock, J. (2007). Using Entropy Analysis to Find Encrypted and Packed Malware. *Ieee Security & Privacy*. https://doi.org/10.1109/msp.2007.48

MADANI, H., OUERDI, N., & Azizi, A. (2023). Ransomware: Analysis of Encrypted Files. *International Journal of Advanced Computer Science and Applications*. https://doi.org/10.14569/ijacsa.2023.0140124

Monaghan, S. M. (2009). Responsible Gambling Strategies for Internet Gambling: The Theoretical and Empirical Base of Using Pop-Up Messages to Encourage Self-Awareness. *Computers in Human Behaviour*. https://doi.org/10.1016/j.chb.2008.08.008

Moser, A., Kruegel, C., & Kirda, E. (2007). *Limits of Static Analysis for Malware Detection*. https://doi.org/10.1109/acsac.2007.21

Naik, N., Jenkins, P., Cooke, R. M., Gillett, J., & Jin, Y. (2020). *Evaluating Automatically Generated YARA Rules and Enhancing Their Effectiveness*. https://doi.org/10.1109/ssci47803.2020.9308179

Nakano, H., Chiba, D., Koide, T., Fukushi, N., Yagi, T., Hariu, T., Yoshioka, K., & Matsumoto, T. (2023). *Canary in Twitter Mine: Collecting Phishing Reports From Experts and Non-Experts*. https://doi.org/10.48550/arxiv.2303.15847

Namanya, A. P., Awan, I.-U., Disso, J. P., & Younas, M. (2020). Similarity Hash Based Scoring of Portable Executable Files for Efficient Malware Detection in IoT. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2019.04.044

Nisa, M., Shah, J. H., Kanwal, S., Raza, M., Khan, M. A., Damaševičius, R., & Blažauskas, T. (2020). Hybrid Malware Classification Method Using Segmentation-Based Fractal Texture Analysis and Deep Convolution Neural Network Features. *Applied Sciences*. https://doi.org/10.3390/app10144966

Nugraha, A., & Zeniarja, J. (2022). Malware Detection Using Decision Tree Algorithm Based on Memory Features Engineering. *Journal of Applied Intelligent System*. https://doi.org/10.33633/jais.v7i3.6735

Oliveira, A. S. d., & Sassi, R. J. (2019). *Behavioural Malware Detection Using Deep Graph Convolutional Neural Networks*. https://doi.org/10.36227/techrxiv.10043099

Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic Malware Analysis in the Modern Era—A State of the Art Survey. *Acm Computing Surveys*. https://doi.org/10.1145/3329786

Pardomuan, C. R., Kurniawan, A., Darus, M. Y., Ariffin, M. A. M., & Muliono, Y. (2023). Server-Side Cross-Site Scripting Detection Powered by HTML Semantic Parsing Inspired by XSS Auditor. *Pertanika Journal of Science and Technology*. https://doi.org/10.47836/pjst.31.3.14

Park, J. S., Sandhu, R., & Ahn, G.-J. (2001). Role-Based Access Control on the Web. *Acm Transactions on Information and System Security*. https://doi.org/10.1145/383775.383777

Putra, A. D., Santoso, J., & Ardiansyah, I. (2022). Analisis Malicious Software Trojan Downloader Pada Android Menggunakan Teknik Reverse Engineering (Studi Kasus: Kamus Kesehatan v2.apk). *Building of Informatics Technology and Science (Bits)*. https://doi.org/10.47065/bits.v4i1.1515

Randhe, V., Chougule, A., & Mukhopadhyay, D. (2013). *Reverse Proxy Framework Using Sanitization Technique for Intrusion Prevention in Database*. https://doi.org/10.1049/cp.2013.2592

Ren, Y., Li, L., & Zhou, J. (2021). *Simtrojan: Stealthy Backdoor Attack*. https://doi.org/10.1109/icip42928.2021.9506313

Rieck, K., Trinius, P., Willems, C., & Holz, T. (2011). Automatic Analysis of Malware Behaviour Using Machine Learning. *Journal of Computer Security*. https://doi.org/10.3233/jcs-2010-0410

Rodriguez, G., Torres, J., Flores, P., & Benavides, D. E. (2020). Cross-Site Scripting (XSS) Attacks and Mitigation: A Survey. *Computer Networks*. https://doi.org/10.1016/j.comnet.2019.106960

Rokkathapa, E., & Kanrar, S. (2019). A Novel Approach for Predicting the Malware Attacks. *International Journal of Computer Applications*. https://doi.org/10.5120/ijca2019918585

Salem, A. H., Backes, M., Ma, S., & Zhang, Y. (2020). *Dynamic Backdoor Attacks Against Machine Learning Models*. https://doi.org/10.48550/arxiv.2003.03675

Salmani, H., Tehranipoor, M., & Plusquellic, J. (2009). *New Design Strategy for Improving Hardware Trojan Detection and Reducing Trojan Activation Time*. https://doi.org/10.1109/hst.2009.5224968

Saprykin, O. S. (2021). Models and Methods for Diagnosing Zero-Daythreats in Cyberspace. *Herald of Advanced Information Technology*. https://doi.org/10.15276/hait.02.2021.5

Shalaginov, A., Banin, S., Dehghantanha, A., & Franke, K. (2018). *Machine Learning Aided Static Malware Analysis: A Survey and Tutorial*. https://doi.org/10.1007/978-3-319-73951-9_2

Shang, W. (2012). *The Sensitive Information Identification for Internet*. https://doi.org/10.2991/emeit.2012.47

Shokr, S. S., & Bahig, H. M. (2022). A Fast Multicore-Based Window Entropy Algorithm. *International Journal of Advanced Computer Science and Applications*. https://doi.org/10.14569/ijacsa.2022.0131127

Sihwail, R., Omar, K., & Ariffin, K. A. Z. (2018). A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis. *International Journal on Advanced Science Engineering and Information Technology*. https://doi.org/10.18517/ijaseit.8.4-2.6827

Souri, A., & Hosseini, R. (2018). A State-of-the-Art Survey of Malware Detection Approaches Using Data Mining Techniques. *Human-Centric Computing and Information Sciences*. https://doi.org/10.1186/s13673-018-0125-x

Srivastava, P., & Raj, M. M. A. (2018). Feature Extraction for Enhanced Malware Detection Using Genetic Algorithm. *International Journal of Engineering & Technology*. https://doi.org/10.14419/ijet.v7i2.8.10479

Srivatanakul, T., & Annansingh, F. (2021). Incorporating Active Learning Activities to the Design and Development of an Undergraduate Software and Web Security Course. *Journal of Computers in Education*. https://doi.org/10.1007/s40692-021-00194-9

S.S., A. K. (2021). SQL Injection Detection Using Machine Learning. *Revista Gestão Inovação E Tecnologias*. https://doi.org/10.47059/revistageintec.v11i3.1939

Stamp, M. (2021). *On Ensemble Learning*. https://doi.org/10.48550/arxiv.2103.12521

Stiawan, D., Bardadi, A., Afifah, N., Melinda, L., Heryanto, A., Septian, T. W., Idris, Mohd. Y., Subroto, I. M. I., Lukman, L., & Budiarto, R. (2023). An Improved LSTM-PCA Ensemble Classifier for SQL Injection and XSS Attack Detection. *Computer Systems Science and Engineering*. https://doi.org/10.32604/csse.2023.034047

Sun, B., Fujino, A., Mori, T., Ban, T., Takahashi, T., & Inoue, D. (2018). Automatically Generating Malware Analysis Reports Using Sandbox Logs. *Ieice Transactions on Information and Systems*. https://doi.org/10.1587/transinf.2017icp0011

Sutriman, & Sugiantoro, B. (2019). Analysis of Password and Salt Combination Scheme to Improve Hash Algorithm Security. *International Journal of*

*Advanced Computer Science and Applications*. https://doi.org/10.14569/ijacsa.2019.0101158

Talukder, S. (2020). *Tools and Techniques for Malware Detection and Analysis*. https://doi.org/10.48550/arxiv.2002.06819

Tetskyi, A. (2023). Тестування На Проникнення Компонентів FPGA Як Сервісу Для Забезпечення Кібербезпеки. *Aerospace Technic and Technology*. https://doi.org/10.32620/aktt.2023.6.11

Torre-Abaitua, G. d. l., Lago-Fernández, L. F., & Arroyo, D. (2021). A Compression-Based Method for Detecting Anomalies in Textual Data. *Entropy*. https://doi.org/10.3390/e23050618

*Tren Judi Online di Indonesia Terus Meningkat, Nilainya Tembus Rp100 T pada 2022*. (n.d.). Retrieved February 20, 2024, from https://databoks.katadata.co.id/datapublish/2023/09/27/tren-judi-online-di-indonesia-terus-meningkat-nilainya-tembus-rp100-t-pada-2022

Tuyishime, E. (2023). Enhancing Cloud Security—Proactive Threat Monitoring and Detection Using a SIEM-Based Approach. *Applied Sciences*. https://doi.org/10.3390/app132212359

Vasudevan, A., & Yerraballi, R. (n.d.). *Stealth Breakpoints*. https://doi.org/10.1109/csac.2005.52

Venkatasubramanian, M., Lashkari, A. H., & Hakak, S. (2023). IoT Malware Analysis Using Federated Learning: A Comprehensive Survey. *Ieee Access*. https://doi.org/10.1109/access.2023.3235389

Venkatraman, S., & Alazab, M. (2018). Use of Data Visualisation for Zero-Day Malware Detection. *Security and Communication Networks*. https://doi.org/10.1155/2018/1728303

Wang, C., Davidson, J. W., Hill, J., & Knight, J. (n.d.). *Protection of Software-Based Survivability Mechanisms*. https://doi.org/10.1109/dsn.2001.941405

Wang, Q., & He, C. (2016). *The Research of an AOP-based Approach to the Detection and Defense of SQL Injection Attack*. https://doi.org/10.2991/aest-16.2016.98

Wassermann, G., & Su, Z. (2008). *Static Detection of Cross-Site Scripting Vulnerabilities*. https://doi.org/10.1145/1368088.1368112

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research*. https://doi.org/10.2196/23692

Yan, J., Qi, Y., & Rao, Q. (2018). Detecting Malware With an Ensemble Method Based on Deep Neural Network. *Security and Communication Networks*. https://doi.org/10.1155/2018/7247095

Ye, Y., Li, T., Zhu, S., Zhuang, W., Tas, E., Gupta, U. C., & Abdulhayoglu, M. (2011). *Combining File Content and File Relations for Cloud Based Malware Detection*. https://doi.org/10.1145/2020408.2020448

Yerima, S. Y., Sezer, S., & Muttik, I. (2015). High Accuracy Android Malware Detection Using Ensemble Learning. *Iet Information Security*. https://doi.org/10.1049/iet-ifs.2014.0099

Yovine, S., Mayr, F., Sosa, S., & Visca, R. (2021). An Assessment of the Application of Private Aggregation of Ensemble Models to Sensible Data.

*Machine Learning and Knowledge Extraction*. https://doi.org/10.3390/make3040039

Yunus, M. A. M., Brohan, M. Z., Nawi, N. M., Surin, E. S. M., Najib, N. A. M., & Liang, C. W. (2018). Review of SQL Injection: Problems and Prevention. *Joiv International Journal on Informatics Visualization*. https://doi.org/10.30630/joiv.2.3-2.144

Zein, M. A., Umar Yunan Kurnia Septo Hediyanto, & Almaarif, A. (2023). Hardening Sistem Operasi Virtual Private Server Fakultas Rekayasa Industri Berdasarkan Nist Sp 800- 123. *Jipi (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*. https://doi.org/10.29100/jipi.v8i1.3438

Zhang, D., Dai, D., Han, R., & Zheng, M. (2021). SentiLog: Anomaly Detecting on Parallel File Systems via Log-based Sentiment Analysis. *Proceedings of the 13th ACM Workshop on Hot Topics in Storage and File Systems*, 86–93.

Zhang, H. (2023). ICVTest: A Practical Black-Box Penetration Testing Framework for Evaluating Cybersecurity of Intelligent Connected Vehicles. *Applied Sciences*. https://doi.org/10.3390/app14010204

Zhang, N., Xue, J., Ma, Y., Zhang, R., Tiancai, L., & Tan, Y. (2021). Hybrid Sequence-based Android Malware Detection Using Natural Language Processing. *International Journal of Intelligent Systems*. https://doi.org/10.1002/int.22529

Zhong, M., Zhou, Y., & Chen, G. (2021). A Security Log Analysis Scheme Using Deep Learning Algorithm for IDSs in Social Network. *Security and Communication Networks*. https://doi.org/10.1155/2021/5542543