

GSJ: Volume 12, Issue 7, July 2024, Online: ISSN 2320-9186

[www.globalscientificjournal.com](http://www.globalscientificjournal.com)











































































































































## REFERENCES

- Abdulrazak, B., Codjo, J. A., & Paul, S. (2022, June). Self-healing approach for IoT architecture: AMI platform. In International Conference on Smart Homes and Health Telematics (pp. 3-17). Cham: Springer International Publishing.
- ABdullah, A., Candrawati, R., & Bhakti, M. A. C. (2009). Multi-Tiered Bio-Inspired Self-Healing Architectural Paradigm for Software Systems. *Jurnal Teknologi Maklumat & Multimedia*, 5, 1-24.
- Alahmadi, B. A. (2019). Malware detection in security operation centres (Doctoral dissertation, University of Oxford).
- Ali, T., & Kostakos, P. (2024). HuntGPT: Integrating Machine Learning-Based Anomaly Detection and Explainable AI with Large Language Models (LLMs). *Journal of Cybersecurity and Networks*, 30(2), 15-29.
- Alt, R., & Puschmann, T. (2012). The rise of customer-oriented banking-electronic markets are paving the way for change in the financial industry. *Electronic Markets*, 22, 203-215.
- Anastopoulos, V., & Giovannelli, D. (2022). Automated/Autonomous Incident Response
- Arzo, S. T., Naiga, C., Granelli, F., Bassoli, R., Devetsikiotis, M., & Fitzek, F. H. (2021). A theoretical discussion and survey of network automation for IoT: Challenges and opportunity. *IEEE Internet of Things Journal*, 8(15), 12021-12045.
- Åström, K. J., & Murray, R. M. (2007). Feedback systems. An Introduction for Scientists and Engineers, Karl Johan Åström and Richard M Murray, 27-64.
- Alyssa. L. (2023, November 29). *How to Perform A Network Stability Test: A Kickass Guide for Network Admins*. <https://obkio.com>. Retrieved April 5, 2024, from <https://obkio.com/blog/network-stability-testing/>
- Barford, P., Kline, J., Plonka, D., & Ron, A. (2002, November). A signal analysis of network traffic anomalies. In Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement (pp. 71-82).
- Bouchama, F., & Kamal, M. (2021). Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns. *International Journal of Business Intelligence and Big Data Analytics*, 4(9), 1-9.
- Burch, Z. C. (2018). Credential Theft Powered Unauthorized Login Detection through Spatial Augmentation (Doctoral dissertation, Virginia Tech).
- Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, 22(1), 616-644.
- Camacho, E. F., Bordons, C., Camacho, E. F., & Bordons, C. (2007). Constrained model predictive control (pp. 177-216). Springer London.
- Carvalho, V. S., Polidoro, M. J., & Magalhaes, J. P. (2016, April). Owlsight: Platform for real-time detection and visualization of cyber threats. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 61-66). IEEE.
- Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. *IEEE Communications Surveys & Tutorials*, 21(3), 2671-2701.
- Cheminod, M., Durante, L., & Valenzano, A. (2012). Review of security issues in industrial networks. *IEEE transactions on industrial informatics*, 9(1), 277-293.
- Chen, P. J., & Chen, Y. W. (2015, September). Implementation of SDN based network intrusion detection and prevention system. In 2015 International Carnahan Conference on Security Technology (ICCST) (pp. 141-146). IEEE.

- Choraś, M., Kozik, R., & Maciejewska, I. (2016). Emerging cyber security: Bio-inspired techniques and MITM detection in IoT. *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*, 193-207.
- Convery, S. (2004). *Network security architectures*. Cisco Press.
- Corradini, I., & Corradini, I. (2020). *The Digital Landscape. Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology*, 1-22.
- Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, 11(10), 4580.
- Eren, H. (2018). *Wireless sensors and instruments: networks, design, and applications*. CRC Press.
- Estévez-Pereira, J. J., Fernández, D., & Novoa, F. J. (2020, August). Network anomaly detection using machine learning techniques. In *Proceedings* (Vol. 54, No. 1, p. 8). MDPI.
- Farzaan, M. A., Ghanem, M. C., & El-Hajjar, A. (2024). AI-Enabled System for Efficient and Effective Cyber Incident Detection and Response in Cloud Environments. arXiv preprint arXiv:2404.05602.
- Fung, H. P. (2014). Criteria, use cases and effects of information technology process automation (ITPA). *Advances in Robotics & Automation*, 3.
- George, A. S., George, A. H., & Baskar, T. (2023). Digitally immune systems: building robust defences in the age of cyber threats. *Partners Universal International Innovation Journal*, 1(4), 155-172.
- González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors*, 21(14), 4759.
- Gracis, R. (2022). *Next Generation SOC: Automations and Machine Learning in Cybersecurity* (Doctoral dissertation, Politecnico di Torino).
- Hossain, M. A., Hussain, I., Al-Athwari, B., & Dahit, S. (2021, June). Network traffic anomalies detection using machine learning algorithm: A performance study. In *International conference on smart computing and cyber security: strategic foresight, security challenges and innovation* (pp. 274-282). Singapore: Springer Nature Singapore.
- Islam, C., Babar, M. A., & Nepal, S. (2019). A multi-vocal review of security orchestration. *ACM Computing Surveys (CSUR)*, 52(2), 1-45.
- Johnphill, O., Sadiq, A. S., Al-Obeidat, F., Al-Khateeb, H., Taheir, M. A., Kaiwartya, O., & Ali, M. (2023). Self-healing in cyber-physical systems using machine learning: A critical analysis of theories and tools. *Future Internet*, 15(7), 244.
- Johnson, M. (2016). *Cyber crime, security and digital intelligence*. Routledge.
- Josyula, V., Orr, M., & Page, G. (2011). *Cloud computing: Automating the virtualized data center*. Cisco Press.
- Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk analysis*, 1(1), 11-27.
- Kara, I. (2023). Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges. *Expert Systems with Applications*, 214, 119133.
- Khan, M. M. I., & Nencioni, G. (2023). Resource Allocation in Networking and Computing Systems: a Security and Dependability Perspective. *IEEE Access*.
- Kirk, D. E. (2004). *Optimal control theory: an introduction*. Courier Corporation.
- Lamnabhi-Lagarrigue, F., Annaswamy, A., Engell, S., Isaksson, A., Khargonekar, P., Murray, R. M., & Van den Hof, P. (2017). Systems & control for the future of humanity, research agenda: Current and future roles, impact and grand challenges. *Annual Reviews in Control*, 43, 1-64.
- Lippmann, R., Webster, S., & Stetson, D. (2002). The effect of identifying vulnerabilities and patching software on the utility of network intrusion detection. In *Recent Advances in Intrusion Detection: 5th International Symposium, RAID 2002 Zurich, Switzerland, October 16-18, 2002 Proceedings 5* (pp. 307-326). Springer Berlin Heidelberg.
- Liu, H., Zhong, C., Alnusair, A., & Islam, S. R. (2021). FAIXID: a framework for enhancing ai explainability of intrusion detection results using data cleaning techniques. *Journal of network and systems management*, 29(4), 40.

- Luenberger, D. G. (1997). Optimization by vector space methods. John Wiley & Sons.
- LeCun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11), 2278-2324.
- Ma, Z., Xiao, M., Xiao, Y., Pang, Z., Poor, H. V., & Vucetic, B. (2019). High-reliability and low-latency wireless communication for internet of things: Challenges, fundamentals, and enabling technologies. *IEEE Internet of Things Journal*, 6(5), 7946-7970.
- Maiello, A. S. (2023). Task Optimization utilizing Digital Transformation Concepts-Automation Project Execution via AGILE Methodology.
- Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. DOI: <https://www.doi.org/10.56726/IRJMETS32644>, 1.
- Mat Isa, M. S. B. (2022). Adaptive Attack Mitigation in Software Defined Networking (Doctoral dissertation, University of Leeds).
- McCulloch, W. S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. *The bulletin of mathematical biophysics*, 5, 115-133.
- Mell, P., Scarfone, K., & Romanosky, S. (2007, June). A complete guide to the common vulnerability scoring system version 2.0. In *Published by FIRST-forum of incident response and security teams (Vol. 1, p. 23)*.
- Mell, P., Kent, K., & Nusbaum, J. (2005). Guide to malware incident prevention and handling (pp. 800-83). Gaithersburg, Maryland: US Department of Commerce, Technology Administration, National Institute of Standards and Technology.
- Meyers, B. S. (2023). Human Error Assessment in Software Engineering. Rochester Institute of Technology.
- Mitchell, T. M. (1997). Artificial neural networks. *Machine learning*, 45(81), 127.
- Mughal, A. A. (2019). Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges. *Applied Research in Artificial Intelligence and Cloud Computing*, 2(1), 1-31.
- Muhati, E., & Rawat, D. (2024). Data-Driven Network Anomaly Detection with Cyber Attack and Defense Visualization. *Journal of Cybersecurity and Privacy*, 4(2), 241-263.
- Muna, E., & Azween, A. (2008). Bio Inspired Intrusion Prevention and Self-healing Architecture for Network Security.
- Müller, O. (2023). RPA-Enabled Security Orchestration: Automating Incident Handling and Remediation. *MZ Computing Journal*, 4(1), 1-7.
- Nankya, M., Chataut, R., & Akl, R. (2023). Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies. *Sensors*, 23(21), 8840.
- Narwal, B., Mohapatra, A. K., & Usmani, K. A. (2019). Towards a taxonomy of cyber threats against target applications. *Journal of Statistics and Management Systems*, 22(2), 301-325.
- Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International Journal of Information Management*, 59, 102334.
- Naseer, H., Desouza, K., Maynard, S. B., & Ahmad, A. (2024). Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics. *European Journal of Information Systems*, 33(2), 200-220.
- Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials*, 21(3), 2702-2733.
- Ochoa-Aday, L., Cervelló-Pastor, C., & Fernández-Fernández, A. (2020). Self-healing and SDN: bridging the gap. *Digital Communications and Networks*, 6(3), 354-368.
- Olaniyi, O. O., Okunleye, O. J., Olabanji, S. O., & Asonze, C. U. (2023). IoT security in the era of ubiquitous computing: A multidisciplinary approach to addressing vulnerabilities and promoting resilience. *Asian Journal of Research in Computer Science*, 16(4).
- Pandey, V. K., De, S., & Nandi, S. (2024). Automated aerial assessment for seamless adaptive adhoc restoration in partially collapsed network. *Computer Communications*, 219, 153-172.

- Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information*. John Wiley & Sons, Inc.
- Pfleeger, C.P., Pfleeger, S.L., & Margulies, J. (2018). *Security in Computing: 5th Edition*.
- Qadir, S., & Quadri, S. M. K. (2016). Information availability: An insight into the most important attribute of information security. *Journal of Information Security*, 7(3), 185-194.
- Rege, P. R., Kalnawat, A., Dhablia, A., Sharma, R., Kaldoke, R. S., & Ashtagi, R. (2024, March). Exploring Machine Learning's Role in Intrusion Detection Systems for Network Security. In *2024 International Conference on Emerging Smart Computing and Informatics (ESCI)* (pp. 1-6). IEEE.
- Rosenblatt, F. (1958). The perceptron: a probabilistic model for information storage and organization in the brain. *Psychological review*, 65(6), 386.
- Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1986). Learning representations by back-propagating errors. *nature*, 323(6088), 533-536.
- Sai, A. P. (2018). *Modeling and Optimization of Dynamical Systems in Epidemiology using Sparse Grid Interpolation*.
- Samek, W., Montavon, G., Vedaldi, A., Hansen, L. K., & Müller, K. R. (Eds.). (2019). *Explainable AI: interpreting, explaining and visualizing deep learning* (Vol. 11700). Springer Nature.
- Scarfone, K., & Hoffman, P. (2009). Guidelines on firewalls and firewall policy. NIST Special Publication, 800(41).
- Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on cyber threat intelligence: The security incident response perspective. *IEEE Communications Surveys & Tutorials*, 23(4), 2525-2556.
- Shah, V. (2021). *Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats*. *Revista Espanola de Documentacion Cientifica*, 15(4), 42-66.
- Sharma, A., Gupta, B. B., Singh, A. K., & Saraswat, V. K. (2023). Advanced Persistent Threats (APT): evolution, anatomy, attribution and countermeasures. *Journal of Ambient Intelligence and Humanized Computing*, 14(7), 9355-9381.
- Shhadih, M. A. (2023). *Cyber Deception Techniques and an Adversary Engagement Platform for Cybersecurity Enhancement* (Doctoral dissertation, The George Washington University).
- Song, W., Beshley, M., Przystupa, K., Beshley, H., Kochan, O., Pryslupskyi, A., & Su, J. (2020). A software deep packet inspection system for network traffic analysis and anomaly detection. *Sensors*, 20(6), 1637.
- Sontan, A. D., & Samuel, S. V. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. *World Journal of Advanced Research and Reviews*, 21(2), 1720-1736.
- Staunton, C. (2020). *Containment through Exploitation: Utilising exploit code to achieve containment and patching of vulnerable systems* (Doctoral dissertation, Letterkenny Institute of Technology).
- Stroeh, K., Mauro Madeira, E. R., & Goldenstein, S. K. (2013). An approach to the correlation of security events based on machine learning techniques. *Journal of Internet Services and Applications*, 4, 1-16.
- Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, 76(12), 9493-9532.
- Taeihagh, A., & Lim, H. S. M. (2019). Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport reviews*, 39(1), 103-128.
- Thapa, M. (2018). *Mitigating Threats in IoT Network Using Device Isolation* (Master's thesis).
- Thapa, S., & Mailewa, A. (2020). The role of intrusion detection/prevention systems in modern computer networks: A review. In *Conference: Midwest Instruction and Computing Symposium (MICS)* (Vol. 53, pp. 1-14).
- Toman, Z. H., Hamel, L., Toman, S. H., Graiet, M., & Valadares, D. C. G. (2024). Formal verification for security and attacks in iot physical layer. *Journal of Reliable Intelligent Environments*, 10(1), 73-91.

- Treider, G. (2023). Investigation of the Gap Between Traditional IP Network Security Management and the Adoption of Automation Techniques and Technologies to Network Security.
- Tripathi, V., Dubey, A., Sathvik, K., & Subhashini, N. (2021, October). A Comparative Study of Machine Learning Algorithms for Anomaly-Based Network Intrusion Detection System. In *International Conference on Computational Techniques and Applications* (pp. 13-21). Singapore: Springer Nature Singapore.
- Usmani, U. A., Happonen, A., & Watada, J. (2022). A review of unsupervised machine learning frameworks for anomaly detection in industrial applications. In *Science and Information Conference* (pp. 158-189). Cham: Springer International Publishing.
- Vasoya, N. H. (2023). Revolutionizing Nano Materials Processing through IoT-AI Integration: Opportunities and Challenges. *Journal of Materials Science Research and Reviews*, 6(3), 294-328.
- Vapnik, V. N., & Vapnik, V. (1998). *Statistical learning theory*.
- Vapnik, V., Golowich, S., & Smola, A. (1996). Support vector method for function approximation, regression estimation and signal processing. *Advances in neural information processing systems*, 9.
- Vasilescu, M., Gheorghe, L., & Tapus, N. (2014, September). Practical malware analysis based on sandboxing. In *2014 RoEduNet Conference 13th Edition: Networking in Education and Research Joint Event RENAM 8th Conference* (pp. 1-6). IEEE.
- Wu, Y. S., Foo, B., Mao, Y. C., Bagchi, S., & Spafford, E. H. (2007). Automated adaptive intrusion containment in systems of interacting services. *Computer networks*, 51(5), 1334-1360.
- Wu, Y. C., Sun, R., & Wu, Y. J. (2020). Smart city development in Taiwan: From the perspective of the information security policy. *Sustainability*, 12(7), 2916.
- Xu, J., & Russello, G. (2022). Automated security-focused network configuration management: State of the art, challenges, and future directions. In *2022 9th international conference on dependable systems and their applications (DSA)* (pp. 409-420). IEEE.
- Ye, Y., Li, T., Adjeroh, D., & Iyengar, S. S. (2017). A survey on malware detection using data mining techniques. *ACM Computing Surveys (CSUR)*, 50(3), 1-40.
- Zeinali, S. M. (2016). *Analysis of security information and event management (SIEM) evasion and detection methods*. Tallinn University of Technology.
- Zhang, Y., Lee, W., & Huang, Y. A. (2003). Intrusion detection techniques for mobile wireless networks. *Wireless Networks*, 9, 545-556.
- Zhang, F., Huff, P., McClanahan, K., & Li, Q. (2020, June). A machine learning-based approach for automated vulnerability remediation analysis. In *2020 IEEE Conference on Communications and Network Security (CNS)* (pp. 1-9). IEEE.
- Zomaya, A. Y., & Lee, Y. C. (Eds.). (2012). *Energy-efficient distributed computing systems*. John Wiley & Sons.