World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Advances in Cybersecurity and AI: Integrating Machine Learning, IoT, and Smart Systems for Resilience and Innovation Across Domains

Yara Shamoo *

Department of Accounting, Saint Leo University, Florida, USA.

World Journal of Advanced Research and Reviews, 2024, 23(02), 2450–2461

Publication history: Received on 18 July 2024; revised on 24 August 2024; accepted on 27 August 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.2.2603

Abstract

Artificial Intelligence (AI) is revolutionizing cybersecurity by offering enhanced threat detection, predictive analytics, and automated responses. However, AI also introduces significant challenges, including bias, lack of transparency, and vulnerability to adversarial attacks. This paper examines the dual role of AI in cybersecurity, providing a comprehensive analysis of its benefits and drawbacks, and discussing the future of AI in securing digital environments.

Keywords: Cybersecurity; Deep Learning; Malware detection; LLMS; AI

1. Introduction

Artificial Intelligence (AI) has rapidly become a transformative force in numerous industries, and cybersecurity is no exception. The rise of cyber threats, ranging from simple phishing attacks to sophisticated state-sponsored hacking campaigns, has necessitated the adoption of more advanced security measures. Traditional cybersecurity methods, which often rely on static rules and signature-based detection, have proven inadequate against the evolving threat landscape. In this context, AI presents itself as a game-changer, offering dynamic and intelligent solutions that can anticipate, detect, and respond to threats with unprecedented speed and accuracy[1-50].

The integration of AI into cybersecurity is driven by its ability to process vast amounts of data, recognize patterns, and learn from experience. Machine learning, a subset of AI, enables systems to improve their performance over time by analyzing historical data and identifying trends. This capability is particularly valuable in cybersecurity, where the nature of threats is constantly changing. For example, AI can analyze network traffic to identify anomalies that may indicate a breach, even if the specific type of attack has never been seen before. This ability to detect zero-day vulnerabilities—those that have not yet been discovered by security researchers—marks a significant advancement over traditional methods.

Another critical area where AI is making an impact is in the automation of responses to detected threats. Cybersecurity operations often involve large amounts of data and require quick decision-making to mitigate risks. AI-driven systems can automate these processes, reducing the time it takes to identify and neutralize threats. For example, AI can automatically block suspicious IP addresses, isolate compromised systems, or revoke user credentials that have been compromised. These automated responses not only improve the speed of incident response but also free up human analysts to focus on more complex tasks that require human judgment and expertise [51-120].

Despite these advantages, the integration of AI into cybersecurity is not without challenges. One of the most significant issues is the potential for bias in AI algorithms. AI systems learn from the data they are trained on, and if this data is biased, the AI's decisions can be skewed. In cybersecurity, this could lead to disproportionate targeting of certain types

* Corresponding author: Yara Shamoo

of behavior or networks, or the overlooking of subtle but significant threats. Moreover, the complexity of AI models, particularly those based on deep learning, makes them difficult to interpret and understand. This 'black box' problem raises concerns about the transparency and accountability of AI-driven decisions, especially in critical areas like cybersecurity.

Another concern is the vulnerability of AI systems to adversarial attacks. These are techniques where attackers manipulate the inputs to an AI system to cause it to make incorrect decisions. In the context of cybersecurity, this could involve tricking an AI system into misclassifying a malicious file as benign, or vice versa. The fact that AI systems can be fooled in this way highlights the need for robust testing and validation of AI models before they are deployed in critical security roles.

The ethical implications of AI in cybersecurity also warrant careful consideration. As AI systems become more autonomous, the question of who is responsible for their decisions becomes increasingly complex. If an AI system incorrectly identifies a legitimate user as a threat and locks them out of a system, who is to blame? The developers of the AI, the organization that deployed it, or the AI itself? These are not just theoretical questions; they have real-world implications for privacy, security, and trust in AI systems.

In conclusion, while AI offers powerful tools for enhancing cybersecurity, it also introduces new risks and challenges that must be carefully managed. The future of AI in cybersecurity will depend on our ability to balance innovation with caution, leveraging AI's strengths while mitigating its weaknesses. As cyber threats continue to evolve, so too must our approaches to combating them, and AI will undoubtedly play a central role in this ongoing battle.

2. Literature Review

The application of AI in cybersecurity has been a subject of extensive research, reflecting the growing recognition of AI's potential to address complex security challenges. Several studies have explored the various ways in which AI can be integrated into cybersecurity frameworks, offering insights into both the opportunities and limitations of this approach [122-144].

One of the most prominent areas of research is the use of machine learning for threat detection and prediction. According to a study by Saleem et al. (2023), machine learning algorithms have been highly effective in identifying patterns of malicious behavior, particularly in detecting previously unknown threats. This study highlights the potential of AI to enhance traditional security measures, particularly in environments where rapid detection of threats is crucial.

Similarly, the work of Gholami and Omar (2023) delves into the application of deep learning in malware analysis. Their research demonstrates that deep learning models, with their ability to process and analyze large volumes of data, are particularly well-suited for identifying subtle indicators of malware that might be missed by conventional detection methods. However, they also note the challenges associated with the black-box nature of deep learning models, which can make it difficult to understand how these systems arrive at their decisions.

Another critical area of research is the use of AI in automating incident response. Basharat and Omar (2024) discuss the development of AI-driven systems that can automatically respond to detected threats, such as by isolating compromised systems or blocking malicious traffic. Their research underscores the potential of AI to reduce the time it takes to respond to security incidents, thereby minimizing damage. However, they also caution that these systems must be carefully monitored to prevent unintended consequences, such as the inadvertent blocking of legitimate users or activities.

Despite the progress in AI research, several challenges remain. The issue of bias in AI systems is a recurring theme in the literature. As Burrell et al. (2022) point out, AI systems are only as good as the data they are trained on, and if this data is biased, the AI's decisions can also be biased. This is particularly concerning in cybersecurity, where biased decisions could lead to unfair treatment of certain users or networks.

The literature also highlights the vulnerability of AI systems to adversarial attacks. Omar and Mohaisen (2022) discuss how attackers can manipulate AI inputs to cause incorrect decisions, a technique known as adversarial attacks. This vulnerability raises significant concerns about the reliability of AI-driven security systems, particularly in high-stakes environments where incorrect decisions could have serious consequences.

3. Opportunities of AI in Cybersecurity

3.1. Enhanced Threat Detection and Response

AI significantly improves threat detection and response by analyzing large datasets from network traffic, system logs, and user behavior. Machine learning algorithms can detect deviations from the norm, identifying potential threats in real-time. This proactive approach is crucial in defending against zero-day attacks and other advanced threats.

3.2. Predictive Analytics

Predictive analytics, powered by AI, enables organizations to anticipate security incidents before they occur. By analyzing historical data, AI can predict future attacks, allowing for proactive defense measures. This predictive capability helps organizations allocate resources more effectively, focusing on the most significant risks.

3.3. Automated Malware Analysis

AI automates the process of malware detection and analysis, reducing the time and effort required for manual analysis. AI systems can detect patterns in malware behavior, even in new or obfuscated samples, making them a powerful tool in combating the ever-evolving threat landscape.

3.4. Case Study: AI in Cloud Security

The adoption of cloud computing has introduced new challenges in cybersecurity. Traditional security measures often struggle to protect cloud environments effectively. AI enhances cloud security by automating threat detection, providing predictive analytics, and enabling rapid response to incidents. This section will explore how AI is being used to secure cloud environments, including its role in identity and access management, data protection, and compliance monitoring.

4. Supplementary Analysis: AI in Cybersecurity

Table 1 Comparative Analysis of AI Techniques in Cybersecurity

AI Technique	Application in Cybersecurity	Advantages	Challenges
Machine Learning	Threat Detection	Fast, Adaptable	Requires large datasets
Deep Learning	Malware Analysis	Accurate, Handles complex patterns	Black-box nature
Predictive Analytics	Risk Management	Proactive, Resource-efficient	Data quality issues
Reinforcement Learning	Autonomous Response	Continuous improvement	Complex to implement

Table 1 provides a comparative analysis of various AI techniques used in cybersecurity. Each technique offers unique advantages and faces specific challenges in its application. For instance, machine learning is effective in threat detection due to its speed and adaptability, but it often requires large datasets to function optimally. On the other hand, deep learning is particularly suited for malware analysis, thanks to its ability to handle complex patterns, though its black-box nature can hinder interpretability.

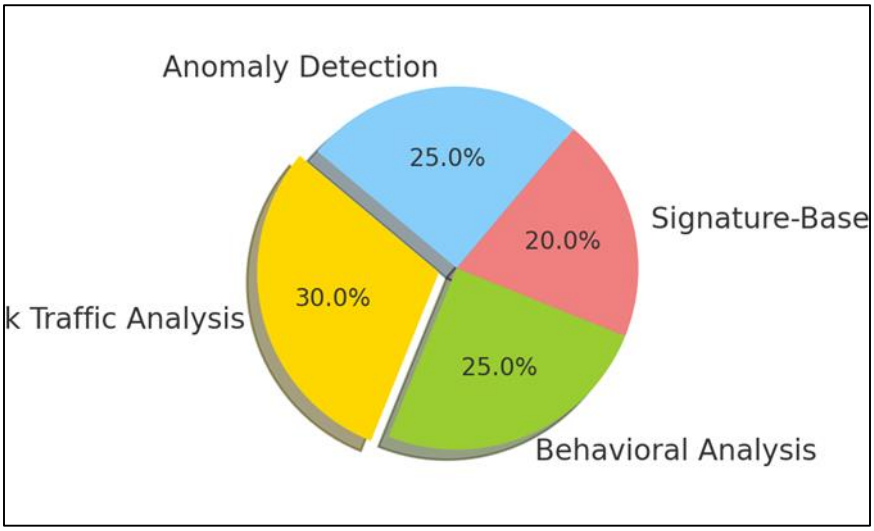

Figure 1 AI's Role in Threat Detection

Figure 1 illustrates the distribution of AI applications in different aspects of threat detection. Network traffic analysis and behavioral analysis represent the largest portions, as AI is increasingly used to identify patterns and anomalies within these data streams. Signature-based detection, although still relevant, is less emphasized in AI-driven systems, which focus more on identifying unknown threats through anomaly detection.

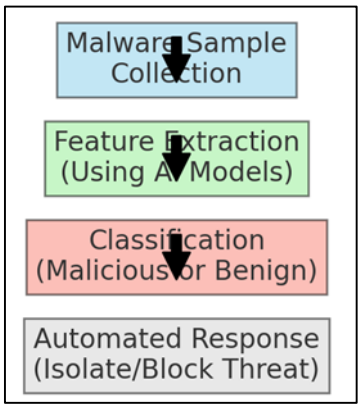

Figure 2 Workflow of AI-Driven Malware Analysis

Figure 2 presents the workflow of AI-driven malware analysis. The process begins with the collection of malware samples, which are then subjected to feature extraction using AI models. These features are analyzed and classified as either malicious or benign. Based on the classification, an automated response is triggered, such as isolating or blocking the identified threat.

5. Challenges of AI in Cybersecurity

5.1. Bias and Fairness

AI systems are susceptible to biases based on the data they are trained on. These biases can lead to unfair or discriminatory outcomes, particularly in security decisions. Addressing these biases is critical to ensure that AI-driven cybersecurity measures are both effective and equitable.

5.2. Interpretability and Transparency

Many AI models, especially those based on deep learning, are often described as 'black boxes' due to their lack of interpretability. In cybersecurity, understanding how AI systems make decisions is crucial for trust and compliance. The complexity of AI models poses challenges in explaining and justifying their actions.

5.3. Adversarial Attacks

AI models are vulnerable to adversarial attacks, where inputs are manipulated to deceive the AI into making incorrect decisions. In cybersecurity, adversarial attacks can lead to false positives or negatives, undermining the effectiveness of AI-driven defenses.

6. Conclusion

AI offers significant advantages in enhancing cybersecurity, from improved threat detection to automated responses and predictive analytics. However, these benefits come with substantial challenges, including bias, lack of transparency, and vulnerability to adversarial attacks. As AI continues to evolve, it is crucial to address these challenges to fully harness its potential in securing digital environments. The future of AI in cybersecurity will depend on balancing innovation with ethical considerations and robust security practices.

Compliance with ethical standards

Disclosure of conflict of interest

All authors have no conflict of interests to declare.

References

[1] Abbasi, R., Bashir, A. K., Mateen, A., Amin, F., Ge, Y., & Omar, M. (2023). Efficient Security and Privacy of Lossless Secure Communication for Sensor-based Urban Cities. *IEEE Sensors Journal*. IEEE.

[2] Ahmed, A., Rasheed, H., Bashir, A. K., & Omar, M. (2023). Millimeter-wave channel modeling in a VANETs using coding techniques. *PeerJ Computer Science*, 9, e1374. PeerJ Inc.

[3] Ahmed, N., Mohammadani, K., Bashir, A. K., Omar, M., Jones, A., & Hassan, F. (2024). Secure and Reliable Routing in the Internet of Vehicles Network: AODV-RL with BHA Attack Defense. *CMES-Computer Modeling in Engineering & Sciences*, 139(1).

[4] Al Harthi, A. S., Al Balushi, M. Y., Al Badi, A. H., Al Karaki, J., & Omar, M. (n.d.). Metaverse Adoption in UAE Higher Education: A Hybrid SEM-ANN Approach..... 98 Mohammad Daradkeh, Boshra Aldhanhani, Amjad Gawanmeh, Shadi Atalla and Sami Miniaoui. *Applied Research Approaches to Technology, Healthcare, and Business*, 1.

[5] Al Kinoon, M., Omar, M., Mohaisen, M., & Mohaisen, D. (2021). Security breaches in the healthcare domain: a spatiotemporal analysis. In *Computational Data and Social Networks: 10th International Conference, CSoNet 2021, Virtual Event, November 15-17, 2021, Proceedings* (pp. 171-183). Springer International Publishing.

[6] Al-Karaki, J. N., Omar, M., Gawanmeh, A., & Jones, A. (2023). Advancing CyberSecurity Education and Training: Practical Case Study of Running Capture the Flag (CTF) on the Metaverse vs. Physical Settings. In *2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA)* (pp. 1-7). IEEE.

[7] Al-Sanjary, O. I., Ahmed, A. A., Jaharadak, A. A. B., Ali, M. A., & Zangana, H. M. (2018, April). Detection clone an object movement using an optical flow approach. In *2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)* (pp. 388-394). IEEE.

[8] Al-Sanjary, O. I., Ahmed, A. A., Zangana, H. M., Ali, M., Aldulaimi, S., & Alkawaz, M. (2018). An investigation of the characteristics and performance of hybrid routing protocol in (MANET). *International Journal of Engineering & Technology*, *7*(4.22), 49-54.

[9] Alturki, N., Altamimi, A., Umer, M., Saidani, O., Alshardan, A., Alsubai, S., Omar, M., & Ashraf, I. (2024). Improving Prediction of Chronic Kidney Disease Using KNN Imputed SMOTE Features and TrioNet Model. *CMES-Computer Modeling in Engineering & Sciences*, 139(3).

[10] Arulappan, A., Raja, G., Bashir, A. K., Mahanti, A., & Omar, M. (2023). ZTMP: Zero Touch Management Provisioning Algorithm for the On-boarding of Cloud-native Virtual Network Functions. *Mobile Networks and Applications*, 1-13. Springer US New York.

[11] Ayub, M. F., Li, X., Mahmood, K., Shamshad, S., Saleem, M. A., & Omar, M. (2023). Secure consumer-centric demand response management in resilient smart grid as industry 5.0 application with blockchain-based authentication. *IEEE Transactions on Consumer Electronics*. IEEE.

[12] Banisakher, M., Mohammed, D., & Omar, M. (2018). A Cloud-Based Computing Architecture Model of Post-Disaster Management System. *International Journal of Simulation--Systems, Science & Technology*, 19(5).

[13] Banisakher, M., Omar, M., & Clare, W. (2019). Critical Infrastructure-Perspectives on the Role of Government in Cybersecurity. *Journal of Computer Sciences and Applications*, 7(1), 37-42.

[14] Banisakher, M., Omar, M., Hong, S., & Adams, J. (2020). A human centric approach to data fusion in post-disaster management. *Journal of Business Management and Science*, 8(1), 12-20.

[15] Basharat, M., & Omar, M. (2024). Adapting to Change: Assessing the Longevity and Resilience of Adversarially Trained NLP Models in Dynamic Spam Detection Environments. In *Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology* (pp. 157-173). IGI Global.

[16] Basharat, M., & Omar, M. (2024). Harnessing GPT-2 for Feature Extraction in Malware Detection: A Novel Approach to Cybersecurity. *Land Forces Academy Review*, 29(1), 74-84.

[17] Basharat, M., & Omar, M. (n.d.). SecuGuard: Leveraging pattern-exploiting training in language models for advanced software vulnerability detection. *International Journal of Mathematics and Computer in Engineering*.

[18] Burrell, D. N., Nobles, C., Cusak, A., Omar, M., & Gillesania, L. (2022). Cybercrime and the Nature of Insider Threat Complexities in Healthcare and Biotechnology Engineering Organizations. *Journal of Crime and Criminal Behavior*, 2(2), 131-144.

[19] Burrell, D. N., Nobles, C., Richardson, K., Wright, J. B., Jones, A. J., Springs, D., & Brown-Jackson, K. (2023). Allison Huff. *Applied Research Approaches to Technology, Healthcare, and Business*, 1. IGI Global.

[20] Davis, L., Dawson, M., & Omar, M. (2016). Systems Engineering Concepts with Aid of Virtual Worlds and Open Source Software: Using Technology to Develop Learning Objects and Simulation Environments. In *Handbook of Research on 3-D Virtual Environments and Hypermedia for Ubiquitous Learning* (pp. 483-509). IGI Global.

[21] Dawson, M. (2015). A brief review of new threats and countermeasures in digital crime and cyber terrorism. *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, 1-7. IGI Global.

[22] Dawson, M., Al Saeed, I., Wright, J., & Omar, M. (2013). Technology enhanced learning with open source software for scientists and engineers. In *INTED2013 Proceedings* (pp. 5583-5589). IATED.

[23] Dawson, M., Davis, L., & Omar, M. (2019). Developing learning objects for engineering and science fields: using technology to test system usability and interface design. *International Journal of Smart Technology and Learning*, 1(2), 140-161. Inderscience Publishers (IEL).

[24] Dawson, M., Eltayeb, M., & Omar, M. (2016). *Security solutions for hyperconnectivity and the Internet of things*. IGI Global.

[25] Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the methods behind cyber terrorism. In *Encyclopedia of Information Science and Technology, Third Edition* (pp. 1539-1549). IGI Global.

[26] Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). *Information security in diverse computing environments*. Academic Press.

[27] Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). The future of national and international security on the internet. In *Information security in diverse computing environments* (pp. 149-178). IGI Global.

[28] Dawson, M., Omar, M., Abramson, J., Leonard, B., & Bessette, D. (2017). Battlefield cyberspace: Exploitation of hyperconnectivity and internet of things. In *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 204-235). IGI Global.

[29] Dawson, M., Wright, J., & Omar, M. (2015). Mobile devices: The case for cyber security hardened systems. In *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 8-29). IGI Global.

[30] Dayoub, A., & Omar, M. (2024). Advancing IoT Security Posture K-Means Clustering for Malware Detection. In *Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology* (pp. 221-239). IGI Global.

[31] Dong, H., Wu, J., Bashir, A. K., Pan, Q., Omar, M., & Al-Dulaimi, A. (2023). Privacy-Preserving EEG Signal Analysis with Electrode Attention for Depression Diagnosis: Joint FHE and CNN Approach. In *GLOBECOM 2023-2023 IEEE Global Communications Conference* (pp. 4265-4270). IEEE.

[32] Fawzi, D., & Omar, M. (n.d.). New insights to database security: An effective and integrated approach to applying access control mechanisms and cryptographic concepts in Microsoft access environments. Academic Press.

[33] Gholami, S. (2024). Can pruning make large language models more efficient? In *Redefining Security With Cyber AI* (pp. 1-14). IGI Global.

[34] Gholami, S. (2024). Do Generative large language models need billions of parameters? In *Redefining Security With Cyber AI* (pp. 37-55). IGI Global.

[35] Gholami, S., & Omar, M. (2023). Does Synthetic Data Make Large Language Models More Efficient? *arXiv preprint arXiv:2310.07830*.

[36] Gholami, S., & Omar, M. (2024). Can a student large language model perform as well as its teacher? In *Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology* (pp. 122-139). IGI Global.

[37] Hamza, Y. A., & Omar, M. D. (2013). Cloud computing security: abuse and nefarious use of cloud computing. *International Journal of Computer Engineering Research*, 3(6), 22-27.

[38] Huff, A. J., Burrell, D. N., Nobles, C., Richardson, K., Wright, J. B., Burton, S. L., Jones, A. J., Springs, D., Omar, M., & Brown-Jackson, K. L. (2023). Management Practices for Mitigating Cybersecurity Threats to Biotechnology Companies, Laboratories, and Healthcare Research Organizations. In *Applied Research Approaches to Technology, Healthcare, and Business* (pp. 1-12). IGI Global.

[39] Jabbari, A., Khan, H., Duraibi, S., Budhiraja, I., Gupta, S., & Omar, M. (2024). Energy Maximization for Wireless Powered Communication Enabled IoT Devices With NOMA Underlaying Solar Powered UAV Using Federated Reinforcement Learning for 6G Networks. *IEEE Transactions on Consumer Electronics*. IEEE.

[40] Jones, A., & Omar, M. (2023). Harnessing the Efficiency of Reformers to Detect Software Vulnerabilities. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 2259-2264). IEEE.

[41] Jones, A., & Omar, M. (2023). Optimized Decision Trees to Detect IoT Malware. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 1761-1765). IEEE.

[42] Jones, A., & Omar, M. (2024). Codesentry: Revolutionizing Real-Time Software Vulnerability Detection With Optimized GPT Framework. *Land Forces Academy Review*, 29(1), 98-107.

[43] Jones, B. M., & Omar, M. (2023). Detection of Twitter Spam with Language Models: A Case Study on How to Use BERT to Protect Children from Spam on Twitter. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 511-516). IEEE.

[44] Jones, B. M., & Omar, M. (2023). Measuring the Impact of Global Health Emergencies on Self-Disclosure Using Language Models. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 1806-1810). IEEE.

[45] Jones, B. M., & Omar, M. (2023). Studying the Effects of Social Media Content on Kids' Safety and Well-being. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 1876-1879). IEEE.

[46] Jones, R., & Omar, M. (2023). Detecting IoT Malware with Knowledge Distillation Technique. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 131-135). IEEE.

[47] Jones, R., & Omar, M. (2024). Codeguard: Utilizing Advanced Pattern Recognition in Language Models for Software Vulnerability Analysis. *Land Forces Academy Review*, 29(1), 108-118.

[48] Jones, R., & Omar, M. (2024). Revolutionizing Cybersecurity: The GPT-2 Enhanced Attack Detection and Defense (GEADD) Method for Zero-Day Threats. *International Journal of Informatics, Information System and Computer Engineering (INJIISCOM)*, 5(2), 178-191.

[49] Jones, R., Omar, M., & Mohammed, D. (2023). Harnessing the Power of the GPT Model to Generate Adversarial Examples. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 1699-1702). IEEE.

[50] Jones, R., Omar, M., Mohammed, D., & Nobles, C. (2023). IoT Malware Detection with GPT Models. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 1749-1752). IEEE.

[51] Jones, R., Omar, M., Mohammed, D., Nobles, C., & Dawson, M. (2023). Harnessing the Speed and Accuracy of Machine Learning to Advance Cybersecurity. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 418-421). IEEE.

[52] Jun, W., Iqbal, M. S., Abbasi, R., Omar, M., & Huiqin, C. (2024). Web-Semantic-Driven Machine Learning and Blockchain for Transformative Change in the Future of Physical Education. *International Journal on Semantic Web and Information Systems (IJSWIS)*, 20(1), 1-16. IGI Global.

[53] Khan, S. A., Alkawaz, M. H., & Zangana, H. M. (2019, June). The use and abuse of social media for spreading fake news. In *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)* (pp. 145-148). IEEE.

[54] Kumar, V. A., Surapaneni, S., Pavitra, D., Venkatesan, R., Omar, M., & Bashir, A. K. (2024). An Internet of Medical Things-Based Mental Disorder Prediction System Using EEG Sensor and Big Data Mining. *Journal of Circuits, Systems and Computers*, 2450197. World Scientific Publishing Company.

[55] Majeed, H. (2020). Watermarking Image Depending on Mojette Transform for Hiding Information. *International Journal Of Computer Sciences And Engineering*, *8*, 8-12.

[56] Mohammed, D., & Omar, M. (2024). Decision Trees Unleashed: Simplifying IoT Malware Detection With Advanced AI Techniques. In *Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology* (pp. 240-258). IGI Global.

[57] Mohammed, D., Omar, M., & Nguyen, V. (2017). Enhancing Cyber Security for Financial Industry through Compliance and Regulatory Standards. In *Security Solutions for Hyperconnectivity and the Internet of Things* (pp. 113-129). IGI Global.

[58] Mohammed, D., Omar, M., & Nguyen, V. (2018). Wireless sensor network security: approaches to detecting and avoiding wormhole attacks. *Journal of Research in Business, Economics and Management*, 10(2), 1860-1864.

[59] Nguyen, V., Mohammed, D., Omar, M., & Banisakher, M. (2018). The Effects of the FCC Net Neutrality Repeal on Security and Privacy. International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), 2(2), 21-29. IGI Global.

[60] Nguyen, V., Mohammed, D., Omar, M., & Dean, P. (2020). Net neutrality around the globe: A survey. In 2020 3rd International Conference on Information and Computer Technologies (ICICT) (pp. 480-488). IEEE.

[61] Nguyen, V., Omar, M., & Mohammed, D. (2017). A Security Framework for Enhancing User Experience. International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), 1(1), 19-28. IGI Global.

[62] Omar, M. & Zangana, H. M. (Eds.). (2024). Redefining Security With Cyber AI. IGI Global. https://doi.org/10.4018/979-8-3693-6517-5

[63] Omar, M. (2012). Smartphone Security: Defending Android-based Smartphone Against Emerging Malware Attacks (Doctoral dissertation, Colorado Technical University).

[64] Omar, M. (2015). Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing. In Handbook of Research on Security Considerations in Cloud Computing (pp. 30-38). IGI Global.

[65] Omar, M. (2015). Insider threats: Detecting and controlling malicious insiders. In New Threats and Countermeasures in Digital Crime and Cyber Terrorism (pp. 162-172). IGI Global.

[66] Omar, M. (2019). A world of cyber attacks (a survey).

[67] Omar, M. (2021). Developing Cybersecurity Education Capabilities at Iraqi Universities.

[68] Omar, M. (2021). New insights into database security: An effective and integrated approach for applying access control mechanisms and cryptographic concepts in Microsoft Access environments.

[69] Omar, M. (2022). Application of machine learning (ML) to address cybersecurity threats. In Machine Learning for Cybersecurity: Innovative Deep Learning Solutions (pp. 1-11). Springer International Publishing Cham.

[70] Omar, M. (2022). Machine Learning for Cybersecurity: Innovative Deep Learning Solutions. Springer Brief. https://link.springer.com/book/978303115

[71] Omar, M. (2022). Malware anomaly detection using local outlier factor technique. In Machine Learning for Cybersecurity: Innovative Deep Learning Solutions (pp. 37-48). Springer International Publishing Cham.

[72] Omar, M. (2023). VulDefend: A Novel Technique based on Pattern-exploiting Training for Detecting Software Vulnerabilities Using Language Models. In 2023 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) (pp. 287-293). IEEE.

[73] Omar, M. (2024). From Attack to Defense: Strengthening DNN Text Classification Against Adversarial Examples. In Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology (pp. 174-195). IGI Global.

[74] Omar, M. (2024). Revolutionizing Malware Detection: A Paradigm Shift Through Optimized Convolutional Neural Networks. In Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology (pp. 196-220). IGI Global.

[75] Omar, M. (n.d.). Defending Cyber Systems through Reverse Engineering of Criminal Malware. Springer Brief. https://link.springer.com/book/9783031116278

[76] Omar, M. (n.d.). Latina Davis Morgan State University 1700 E Cold Spring Ln. Baltimore, MD 21251, USA E-mail: latinaedavis@ hotmail. com.

[77] Omar, M. (n.d.). Machine Learning for Cybersecurity.

[78] Omar, M., & Burrell, D. (2023). From text to threats: A language model approach to software vulnerability detection. International Journal of Mathematics and Computer in Engineering.

[79] Omar, M., & Burrell, D. N. (2024). Organizational Dynamics and Bias in Artificial Intelligence (AI) Recruitment Algorithms. In Evolution of Cross-Sector Cyber Intelligent Markets (pp. 269-290). IGI Global.

[80] Omar, M., & Dawson, M. (2013). Research in progress-defending android smartphones from malware attacks. In 2013 third international conference on advanced computing and communication technologies (ACCT) (pp. 288-292). IEEE.

[81] Omar, M., & Mohaisen, D. (2022). Making Adversarially-Trained Language Models Forget with Model Retraining: A Case Study on Hate Speech Detection. In Companion Proceedings of the Web Conference 2022 (pp. 887-893).

[82] Omar, M., & Shiaeles, S. (2023). VulDetect: A novel technique for detecting software vulnerabilities using Language Models. In 2023 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE. https://ieeexplore.ieee.org/document/10224924

[83] Omar, M., & Sukthankar, G. (2023). Text-defend: detecting adversarial examples using local outlier factor. In 2023 IEEE 17th international conference on semantic computing (ICSC) (pp. 118-122). IEEE.

[84] Omar, M., Bauer, R., Fernando, A., Darejeh, A., Rahman, S., Ulusoy, S. K., Arabo, A., Gupta, R., Adedoyin, F., Paul, R. K., & others. (2024). Committee Members. In Journal of Physics: Conference Series, 2711, 011001.

[85] Omar, M., Choi, S., Nyang, D., & Mohaisen, D. (2022). Quantifying the performance of adversarial training on language models with distribution shifts. In Proceedings of the 1st Workshop on Cybersecurity and Social Sciences (pp. 3-9).

[86] Omar, M., Choi, S., Nyang, D., & Mohaisen, D. (2022). Robust natural language processing: Recent advances, challenges, and future directions. IEEE Access, 10, 86038-86056. IEEE.

[87] Omar, M., Gouveia, L. B., Al-Karaki, J., & Mohammed, D. (2022). Reverse-Engineering Malware. In Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security (pp. 194-217). IGI Global.

[88] Omar, M., Jones, R., Burrell, D. N., Dawson, M., Nobles, C., & Mohammed, D. (2023). Harnessing the power and simplicity of decision trees to detect IoT Malware. In Transformational Interventions for Business, Technology, and Healthcare (pp. 215-229). IGI Global.

[89] Omar, M., Mohammed, D., & Nguyen, V. (2017). Defending against malicious insiders: a conceptual framework for predicting, detecting, and deterring malicious insiders. International Journal of Business Process Integration and Management, 8(2), 114-119. Inderscience Publishers (IEL).

[90] Omar, M., Mohammed, D., Nguyen, V., Dawson, M., & Banisakher, M. (2021). Android application security. In Research Anthology on Securing Mobile Technologies and Applications (pp. 610-625). IGI Global.

[91] Pauu, K. T., Pan, Q., Wu, J., Bashir, A. K., & Omar, M. (2024). IRS-Aided Federated Learning with Dynamic Differential Privacy for UAVs in Emergency Response. IEEE Internet of Things Magazine, 7(4), 108-115. IEEE.

[92] Peng, Y., Wang, J., Ye, X., Khan, F., Bashir, A. K., Alshawi, B., Liu, L., & Omar, M. (2024). An intelligent resource allocation strategy with slicing and auction for private edge cloud systems. Future Generation Computer Systems, 160, 879-889. North-Holland.

[93] Rajesh, R., Hemalatha, S., Nagarajan, S. M., Devarajan, G. G., Omar, M., & Bashir, A. K. (2024). Threat Detection and Mitigation for Tactile Internet Driven Consumer IoT-Healthcare System. IEEE Transactions on Consumer Electronics. IEEE.

[94] Saleem, M. A., Li, X., Mahmood, K., Shamshad, S., Ayub, M. F., & Omar, M. (2023). Provably secure conditional-privacy access control protocol for intelligent customers-centric communication in vanet. IEEE Transactions on Consumer Electronics. IEEE.

[95] Sun, Y., Xu, T., Bashir, A. K., Liu, J., & Omar, M. (2023). BcIIS: Blockchain-Based Intelligent Identification Scheme of Massive IoT Devices. In GLOBECOM 2023-2023 IEEE Global Communications Conference (pp. 1277-1282). IEEE.

[96] Tao, Y., Wu, J., Pan, Q., Bashir, A. K., & Omar, M. (2024). O-RAN-Based Digital Twin Function Virtualization for Sustainable IoV Service Response: An Asynchronous Hierarchical Reinforcement Learning Approach. IEEE Transactions on Green Communications and Networking. IEEE.

[97] Tiwari, N., Ghadi, Y., & Omar, M. (2023). Analysis of Ultrasound Images in Kidney Failure Diagnosis Using Deep Learning. In Transformational Interventions for Business, Technology, and Healthcare (pp. 45-74). IGI Global.

[98] Tiwari, N., Omar, M., & Ghadi, Y. (2023). Brain Tumor Classification From Magnetic Resonance Imaging Using Deep Learning and Novel Data Augmentation. In Transformational Interventions for Business, Technology, and Healthcare (pp. 392-413). IGI Global.

[99] Umer, M., Aljrees, T., Karamti, H., Ishaq, A., Alsubai, S., Omar, M., Bashir, A. K., & Ashraf, I. (2023). Heart failure patients monitoring using IoT-based remote monitoring system. Scientific Reports, 13(1), 19213. Nature Publishing Group UK London.

[100] Wright, J., Dawson Jr, M. E., & Omar, M. (2012). Cyber security and mobile threats: The need for antivirus applications for smartphones. Journal of Information Systems Technology and Planning, 5(14), 40-60.

[101] Xu, X., Wu, J., Bashir, A. K., & Omar, M. (2024). Machine Learning and Zero Knowledge Empowered Trustworthy Bitcoin Mixing for Next-G Consumer Electronics Payment. IEEE Transactions on Consumer Electronics. IEEE.

[102] Zangana, H. M. (2015). A New Skin Color Based Face Detection Algorithm by Combining Three Color Model Algorithms. IOSR J. Comput. Eng, 17, 06-125.

[103] Zangana, H. M. (2017). A new algorithm for shape detection. IOSR Journal of Computer Engineering (IOSR-JCE), 19(3), 71-76.

[104] Zangana, H. M. (2017). Library Data Quality Maturity (IIUM as a Case Study). IOSR-JCE March, 29, 2017.

[105] Zangana, H. M. (2017). Watermarking System Using LSB. IOSR Journal of Computer Engineering, 19(3), 75-79.

[106] Zangana, H. M. (2018). Design an information management system for a pharmacy. International Journal of Advanced Research in Computer and Communication Engineering, 7(10).

[107] Zangana, H. M. (2018). Developing Data Warehouse for Student Information System (IIUM as a Case Study). International Organization of Scientific Research, 20(1), 09-14.

[108] Zangana, H. M. (2018). Developing Data Warehouse for Student Information System (IIUM as a Case Study). International Organization of Scientific Research, 20(1), 09-14.

[109] Zangana, H. M. (2018). Implementing a System for Recognizing Optical Characters.

[110] Zangana, H. M. (2019). Issues of Data Management in the Library: A Case Study.

[111] Zangana, H. M. (2019). ITD Data Quality Maturity (A Case Study). International Journal Of Engineering And Computer Science, 8(10).

[112] Zangana, H. M. (2020). Mobile Device Integration in IIUM Service. International Journal, 8(5).

[113] Zangana, H. M. (2021). The Global Finical Crisis from an Islamic Point Of View. Qubahan Academic Journal, 1(2), 55-59.

[114] Zangana, H. M. (2022). Creating a Community-Based Disaster Management System. Academic Journal of Nawroz University, 11(4), 234-244.

[115] Zangana, H. M. (2022). Implementing New Interactive Video Learning System for IIUM. Academic Journal of Nawroz University, 11(2), 23-29.

[116] Zangana, H. M. (2022). Improving The Web Services for Remittance Company: Express Remit as a Case Study. Academic Journal of Nawroz University (AJNU), 11(3).

[117] Zangana, H. M. (2024). Exploring Blockchain-Based Timestamping Tools: A Comprehensive Review. Redefining Security With Cyber AI, 92-110.

[118] Zangana, H. M. (2024). Exploring the Landscape of Website Vulnerability Scanners: A Comprehensive Review and Comparative Analysis. Redefining Security With Cyber AI, 111-129.

[119] Zangana, H. M. CHALLENGES AND ISSUES of MANET.

[120] Zangana, H. M., & Abdulazeez, A. M. (2023). Developed Clustering Algorithms for Engineering Applications: A Review. International Journal of Informatics, Information System and Computer Engineering (INJIISCOM), 4(2), 147-169.

[121] Zangana, H. M., & Al-Shaikhli, I. F. (2013). A new algorithm for human face detection using skin color tone. IOSR Journal of Computer Engineering, 11(6), 31-38.

[122] Zangana, H. M., & Mustafa, F. M. (2024). From Classical to Deep Learning: A Systematic Review of Image Denoising Techniques. Jurnal Ilmiah Computer Science, 3(1), 50-65.

[123] Zangana, H. M., & Mustafa, F. M. (2024). Review of Hybrid Denoising Approaches in Face Recognition: Bridging Wavelet Transform and Deep Learning. The Indonesian Journal of Computer Science, 13(4).

[124] Zangana, H. M., & Mustafa, F. M. (2024). Surveying the Landscape: A Comprehensive Review of Object Detection Algorithms and Advancements. Jurnal Ilmiah Computer Science, 3(1), 1-15.

[125] Zangana, H. M., & Omar, M. (2020). Threats, Attacks, and Mitigations of Smartphone Security. Academic Journal of Nawroz University, 9(4), 324-332.

[126] Zangana, H. M., & Omar, M. (2020). Threats, Attacks, and Mitigations of Smartphone Security. Academic Journal of Nawroz University, 9(4), 324-332.

[127] Zangana, H. M., & Zeebaree, S. R. (2024). Distributed Systems for Artificial Intelligence in Cloud Computing: A Review of AI-Powered Applications and Services. International Journal of Informatics, Information System and Computer Engineering (INJIISCOM), 5(1), 11-30.

[128] Zangana, H. M., Al-Shaikhli, I. F., & Graha, Y. I. (2013). The Ethical Dilemma of Software Piracy: An Inquiry from an Islamic Perspective. Creative Communication and Innovative Technology Journal, 7(1), 59-76.

[129] Zangana, H. M., Bazeed, S. M. S., Ali, N. Y., & Abdullah, D. T. (2024). Navigating Project Change: A Comprehensive Review of Change Management Strategies and Practices. Indonesian Journal of Education and Social Sciences, 3(2), 166-179.

[130] Zangana, H. M., Graha, Y. I., & Al-Shaikhli, I. F. Blogging: A New Platform For Spreading Rumors!. Creative Communication and Innovative Technology Journal, 9(1), 71-76.

[131] Zangana, H. M., khalid Mohammed, A., & Zeebaree, S. R. (2024). Systematic Review of Decentralized and Collaborative Computing Models in Cloud Architectures for Distributed Edge Computing. Sistemasi: Jurnal Sistem Informasi, 13(4), 1501-1509.

[132] Zangana, H. M., Mohammed, A. K., & Mustafa, F. M. (2024). Advancements and Applications of Convolutional Neural Networks in Image Analysis: A Comprehensive Review. Jurnal Ilmiah Computer Science, 3(1), 16-29.

[133] Zangana, H. M., Mohammed, A. K., & Mustafa, F. M. (2024). Advancements in Edge Detection Techniques for Image Enhancement: A Comprehensive Review. International Journal of Artificial Intelligence & Robotics (IJAIR), 6(1), 29-39.

[134] Zangana, H. M., Mohammed, A. K., Sallow, A. B., & Sallow, Z. B. (2024). Cybernetic Deception: Unraveling the Layers of Email Phishing Threats. International Journal of Research and Applied Technology (INJURATECH), 4(1), 35-47.

[135] Zangana, H. M., Mohammed, A. K., Sallow, Z. B., & Mustafa, F. M. (2024). Exploring Image Representation and Color Spaces in Computer Vision: A Comprehensive Review. The Indonesian Journal of Computer Science, 13(3).

[136] Zangana, H. M., Natheer Yaseen Ali, & Ayaz khalid Mohammed. (2024). Navigating the Digital Marketplace: A Comprehensive Review of E-Commerce Trends, Challenges, and Innovations. TIJAB (The International Journal of Applied Business), 8(1), 88–103. https://doi.org/10.20473/tijab.v8.I1.2024.54618

[137] Zangana, H. M., Omar, M., Al-Karaki, J. N., & Mohammed, D. (2024). Comprehensive Review and Analysis of Network Firewall Rule Analyzers: Enhancing Security Posture and Efficiency. Redefining Security With Cyber AI, 15-36.

[138] Zangana, H. M., Omar, M., Al-Karaki, J. N., & Mohammed, D. (2024). Comprehensive Review and Analysis of Network Firewall Rule Analyzers: Enhancing Security Posture and Efficiency. In Redefining Security With Cyber AI (pp. 15-36). IGI Global.

[139] Zangana, H. M., Sallow, Z. B., Alkawaz, M. H., & Omar, M. (2024). Unveiling the Collective Wisdom: A Review of Swarm Intelligence in Problem Solving and Optimization. Inform: Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi, 9(2), 101-110.

[140] Zangana, H. M., Sallow, Z. B., Alkawaz, M. H., & Omar, M. (2024). Unveiling the Collective Wisdom: A Review of Swarm Intelligence in Problem Solving and Optimization. Inform: Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi, 9(2), 101-110.

[141] Zangana, H. M., Tawfiq, N. E., & Omar, M. (2020). Advantages and Challenges of E-Government in Turkey.

[142] Zangana[1], H. M., Tawfiq, N. E., & Omar, M. (2020). Advantages and Challenges of E-Government in Turkey.

[143] Zhang, H., Wu, J., Pan, Q., Bashir, A. K., & Omar, M. (2024). Toward Byzantine-Robust Distributed Learning for Sentiment Classification on Social Media Platform. IEEE Transactions on Computational Social Systems. IEEE.

[144] Zhou, S., Ali, A., Al-Fuqaha, A., Omar, M., & Feng, L. (n.d.). Robust Risk-Sensitive Task Offloading for Edge-Enabled Industrial Internet of Things. IEEE Transactions on Consumer Electronics.