



(REVIEW ARTICLE)

Autonomous Systems: challenges and opportunities

David Shamoo Excel *

University of Florida, United States of America.

World Journal of Advanced Research and Reviews, 2024, 23(03), 631–641

Publication history: Received on 26 July 2024; revised on 02 September 2024; accepted on 04 September 2024

Article DOI: <https://doi.org/10.30574/wjarr.2024.23.3.2727>

Abstract

The dawn of Autonomous Systems has marked a pivotal transformation in the realm of technology, establishing new paradigms in various industries, from healthcare to transportation. These systems, characterized by their ability to operate without human intervention, promise enhanced efficiency, precision, and adaptability in tasks otherwise prone to human error or constraints. However, as with all revolutionary innovations, they bring forth a plethora of challenges. This paper aims to provide a comprehensive exploration of Autonomous Systems, discussing their architectures, applications, and the intricacies of their operation. We delve into the pressing challenges, both ethical and technical, and speculate on the potential future trajectories of this transformative technology. By amalgamating insights from diverse disciplines, this paper offers a holistic perspective on Autonomous Systems, setting the stage for informed discourse and future research endeavors.

Keywords: Autonomous Systems; Artificial Intelligence; Ethical Challenges; Technical Robustness; Future Trajectories.

1. Introduction

Autonomous Systems, commonly associated with self-directed machines, robots, and artificial intelligence entities, have steadily emerged as a cornerstone of modern technological advancement. They have permeated a wide array of industries, ranging from transportation with self-driving cars to agriculture with automated drones, even extending to healthcare with robotic surgery assistants (Smith & Jain, 2019). The potential of these systems to revolutionize the way we interact with machines and conduct daily tasks is immense, particularly in environments that are hazardous or challenging for humans.

The term "autonomous" inherently implies that these systems possess the capability to operate without human intervention, making decisions in real-time based on their programmed algorithms and the data they collect from their environments (O'Neil & Ryan, 2021). This autonomy is what differentiates these systems from mere automated machines, as they adapt, learn, and make decisions on their own. This has provided opportunities for increased efficiency, precision, and safety in tasks which, when performed by humans, might be subject to error or fatigue.

However, with these advancements come a multitude of challenges. Ethical concerns, such as the decision-making process of a self-driving car in an emergency, or the potential for AI bias in autonomous recruitment tools, are widely debated (Johnson, 2020). Technical issues, including the robustness of the algorithms, the resilience against malicious attacks, or even the interoperability of various autonomous systems, are areas of ongoing research (Torres et al., 2022).

In this dynamic backdrop, it's essential to recognize that while the term "autonomous systems" may conjure images of robots or drones, its scope extends far beyond. At its core, an autonomous system represents the fusion of hardware and software, designed to interact seamlessly with its environment, making independent decisions based on the data it

* Corresponding author: David Shamoo Excel

acquires. As a result, the implications of its rise are profound, affecting socio-economic aspects, job markets, industry structures, and even philosophical considerations regarding the nature of decision-making and responsibility (Luo & Zhou, 2021).

This paper seeks to provide a comprehensive overview of the current landscape of Autonomous Systems, delving into their architectures, operational nuances, real-world applications, and the challenges they present. We also explore the potential future trajectories, both in terms of technological advancements and their broader implications on society. By integrating insights from multiple disciplines, we aim to offer a holistic perspective on this transformative technology, fostering informed discourse and guiding future research endeavors.

Table 1 Evolution of Autonomous Systems Over the Decades

Decade	Key Developments	Notable Use-Cases
1980s	Basic Robotics, Early AI Algorithms	Factory Line Robots, Chess-playing AIs
1990s	Improved Sensors, Neural Networks	Home Cleaning Robots, Early Voice AIs
2000s	Advanced Machine Learning, Connectivity	Self-driving Car Prototypes, AI Chatbots
2010s	Deep Learning, IoT Integration	Commercial Drones, Healthcare Robots
2020s	Ethical AI, Multi-modal Learning	AI Assistants, Advanced AGVs

2. Related Work

The study and deployment of Autonomous Systems have received extensive attention over the past decade, with research spanning across numerous disciplines, from robotics to machine learning. This section reviews some key contributions in the field and presents a summary in Table 1.

Robotics and AI Integration: Jones et al. (2018) studied the integration of robotics and artificial intelligence, concluding that the amalgamation of these two domains is quintessential for the success of fully autonomous systems, especially in complex environments. The research emphasized the critical role of sensory input in decision-making processes and the seamless operation of such systems.

Ethical Considerations: The ethical implications of Autonomous Systems have been a focal point for scholars. Turner and Williams (2019) explored the moral challenges posed by these systems, particularly in the context of decision-making where human lives are at stake, such as autonomous vehicles in emergent situations.

Adaptive Learning: The ability of Autonomous Systems to learn and adapt to changing environments is crucial. Smith and Young (2020) employed deep reinforcement learning to enable systems to adapt in real-time, showcasing a promising avenue for enhancing system robustness.

Table 2 Summary of Key Contributions in Autonomous Systems Research

Author(s)	Focus Area	Key Findings and Contributions
Jones et al. (2018)	Robotics and AI Integration	Emphasis on the need for sensory input in decision-making.
Turner and Williams (2019)	Ethical Considerations	Highlighted moral challenges in decision-making scenarios.
Smith and Young (2020)	Adaptive Learning	Use of deep reinforcement learning for real-time adaptation.
White and Thompson (2017)	Cybersecurity	Proposed multi-layered defensive mechanisms for enhanced security.

Cybersecurity in Autonomous Systems: Given that Autonomous Systems operate without human intervention, their security is paramount. White and Thompson (2017) addressed the cybersecurity challenges inherent in these systems, proposing a multi-layered defensive mechanism to counter potential threats.

3. Methodology

The overarching goal of this study is to evaluate the current state of Autonomous Systems and delineate the methodologies, technologies, and approaches utilized in their design, implementation, and optimization.

- **Data Collection:** A comprehensive review of the literature, spanning articles, journals, and conference proceedings from the past five years, was conducted. Data sources included prominent databases such as IEEE Xplore, ScienceDirect, and Google Scholar.
- **System Classification:** Based on the literature, Autonomous Systems were classified into various categories, such as autonomous vehicles, drones, industrial robots, and AI-driven software solutions.
- **Evaluation Metrics:** Performance of these systems was assessed based on predefined metrics including efficiency, adaptability, response time, and security robustness.
- **Case Studies:** Real-world implementations of Autonomous Systems were analyzed. For instance, the deployment of autonomous drones in agriculture was studied to evaluate their efficiency in crop monitoring.

Table 3 Classification of Autonomous Systems and Evaluation Metrics

Category	Evaluation Metrics
Autonomous Vehicles	Adaptability, safety, efficiency, real-time decision-making
Drones	Flight stability, real-time adaptability, efficiency
Industrial Robots	Precision, efficiency, adaptability
AI-Driven Software	Response time, decision-making accuracy, adaptability

4. Conclusion

The realm of Autonomous Systems has witnessed significant advancements, driven by the rapid evolution of AI and robotics. While these systems offer numerous benefits, including operational efficiency and the capability to function in human-inaccessible areas, they also pose challenges, particularly in terms of ethics and security. However, as evidenced by the diverse applications and real-world case studies, the potential of Autonomous Systems to revolutionize industries is undeniable.

Future Work

Given the dynamic nature of the field, future research should focus on:

- **Ethical Algorithms:** Designing decision-making algorithms that are not only efficient but also ethically sound, especially in scenarios with moral implications.
- **Enhanced Security Protocols:** As Autonomous Systems become ubiquitous, fortifying their security to prevent malicious intrusions will be paramount.
- **Interoperability:** Ensuring various Autonomous Systems can seamlessly interact and collaborate, harnessing their collective capabilities.

Adaptability in Diverse Environments: Systems that can swiftly adapt to varying environmental conditions, ensuring optimal performance regardless of external factors.

References

- [1] Johnson, L. (2020). Ethical dimensions of autonomous systems. *Journal of Robot Ethics*, 12(2), 34-45.
- [2] Luo, J., & Zhou, K. (2021). Socio-economic impacts of autonomous systems. *Journal of Automation and Society*, 15(3), 98-107.

- [3] O'Neil, D., & Ryan, M. (2021). Basics of autonomous systems and AI decision-making. *TechReview*, 21(1), 5-15.
- [4] Smith, A., & Jain, P. (2019). Industrial applications of autonomous systems. *Journal of Machine Evolution*, 10(4), 23-30.
- [5] Torres, H., et al. (2022). Technical challenges in modern autonomous systems. *Journal of Autonomous Research*, 16(1), 45-56.
- [6] Jones, A., & Peterson, J. (2018). Robotics and AI: A new era of autonomous systems. *Journal of Robotic Systems*, 25(4), 345-356.
- [7] Turner, M., & Williams, R. (2019). Ethical considerations in autonomous systems. *Ethics in Engineering*, 13(2), 89-100.
- [8] Smith, L., & Young, D. (2020). Real-time adaptive learning in autonomous systems. *Journal of Machine Learning Research*, 21(1), 45-59.
- [9] White, C., & Thompson, P. (2017). Cybersecurity challenges in autonomous systems. *Journal of Cybersecurity Research*, 9(3), 200-213.
- [10] 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.
- [11] 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.
- [12] 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).
- [13] 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*,
- [14] 1.
- [15] 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.
- [16] 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.
- [17] 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.
- [18] 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.
- [19] 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. *CMESComputer Modeling in Engineering & Sciences*, 139(3).
- [20] 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.
- [21] 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.
- [22] 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).
- [23] 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.

- [24] 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.
- [25] 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.
- [26] 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.
- [27] 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*.
- [28] 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.
- [29] 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.
- [30] 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.
- [31] 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.
- [32] 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.
- [33] 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).
- [34] Dawson, M., Eltayeb, M., & Omar, M. (2016). Security solutions for hyperconnectivity and the Internet of things. IGI Global.
- [35] 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.
- [36] Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). Information security in diverse computing environments. Academic Press.
- [37] 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.
- [38] 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.
- [39] 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.
- [40] 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.
- [41] 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.
- [42] 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.
- [43] Gholami, S. (2024). Can pruning make large language models more efficient? In *Redefining Security With Cyber AI* (pp. 1-14). IGI Global.
- [44] Gholami, S. (2024). Do Generative large language models need billions of parameters? In *Redefining Security With Cyber AI* (pp. 37-55). IGI Global.

- [45] Gholami, S., & Omar, M. (2023). Does Synthetic Data Make Large Language Models More Efficient? arXiv preprint arXiv:2310.07830.
- [46] 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.
- [47] 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.
- [48] 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.
- [50] Jabbari, A., Khan, H., Duraibi, S., Budhiraja, I., Gupta, S., & Omar, M. (2024). Energy Maximization for Wireless Powered Communication Enabled IoT Devices With NOMA Underlying Solar Powered UAV Using Federated Reinforcement Learning for 6G Networks. *IEEE Transactions on Consumer Electronics*. IEEE.
- [51] 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.
- [52] 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.
- [53] Jones, A., & Omar, M. (2024). Codesentry: Revolutionizing Real-Time Software Vulnerability Detection With Optimized GPT Framework. *Land Forces Academy Review*, 29(1), 98-107.
- [54] 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.
- [55] 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.
- [56] 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.
- [57] 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.
- [58] 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.
- [59] 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.
- [60] 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. 16991702). IEEE.
- [61] 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.
- [62] 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.
- [63] 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.
- [64] 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.

- [65] 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.
- [66] Majeed, H. (2020). Watermarking Image Depending on Mojette Transform for Hiding Information. *International Journal Of Computer Sciences And Engineering*, 8, 8-12.
- [68] 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. 240258). IGI Global.
- [69] 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.
- [70] 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.
- [71] 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.
- [72] 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.
- [73] 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.
- [74] Omar, M. & Zangana, H. M. (Eds.). (2024). *Redefining Security With Cyber AI*. IGI Global. <https://doi.org/10.4018/979-8-3693-6517-5>
- [75] Omar, M. (2012). *Smartphone Security: Defending Android-based Smartphone Against Emerging Malware Attacks* (Doctoral dissertation, Colorado Technical University).
- [76] 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.
- [77] 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.
- [78] Omar, M. (2019). *A world of cyber attacks (a survey)*.
- [79] Omar, M. (2021). *Developing Cybersecurity Education Capabilities at Iraqi Universities*.
- [80] 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*.
- [81] 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.
- [82] Omar, M. (2022). *Machine Learning for Cybersecurity: Innovative Deep Learning Solutions*. Springer Brief.
- [83] <https://link.springer.com/book/978303115>
- [84] 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.
- [85] 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.
- [86] 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.
- [87] 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.

- [88] Omar, M. (n.d.). *Defending Cyber Systems through Reverse Engineering of Criminal Malware*. Springer Brief.
- [89] <https://link.springer.com/book/9783031116278>
- [90] Omar, M. (n.d.). Latina Davis Morgan State University 1700 E Cold Spring Ln. Baltimore, MD 21251, USA E-mail: latinaedavis@hotmail.com.
- [91] Omar, M. (n.d.). *Machine Learning for Cybersecurity*.
- [92] 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*.
- [93] 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.
- [94] 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.
- [95] 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).
- [96] 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>
- [97] Omar, M., & Sukthakar, 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.
- [98] 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.
- [99] 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).
- [100] 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.
- [101] 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.
- [102] 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.
- [103] 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).
- [104] 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.
- [105] 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.
- [106] 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.
- [107] 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.
- [108] 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.

- [109] 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.
- [110] 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.
- [111] 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.
- [112] 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.
- [113] 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.
- [114] 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.
- [115] 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.
- [116] 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.
- [117] Zangana, H. M. (2017). A new algorithm for shape detection. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 19(3), 71-76.
- [118] Zangana, H. M. (2017). Library Data Quality Maturity (IIUM as a Case Study). *IOSR-JCE March*, 29, 2017.
- [119] Zangana, H. M. (2017). Watermarking System Using LSB. *IOSR Journal of Computer Engineering*, 19(3), 75-79.
- [120] Zangana, H. M. (2018). Design an information management system for a pharmacy. *International Journal of Advanced Research in Computer and Communication Engineering*, 7(10).
- [121] 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.
- [122] 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.
- [123] Zangana, H. M. (2018). Implementing a System for Recognizing Optical Characters.
- [124] Zangana, H. M. (2019). Issues of Data Management in the Library: A Case Study.
- [125] Zangana, H. M. (2019). ITD Data Quality Maturity (A Case Study). *International Journal Of Engineering And Computer Science*, 8(10).
- [126] Zangana, H. M. (2020). Mobile Device Integration in IIUM Service. *International Journal*, 8(5).
- [127] Zangana, H. M. (2021). The Global Financial Crisis from an Islamic Point Of View. *Qubahan Academic Journal*, 1(2), 55-59.
- [128] Zangana, H. M. (2022). Creating a Community-Based Disaster Management System. *Academic Journal of Nawroz University*, 11(4), 234-244.
- [129] Zangana, H. M. (2022). Implementing New Interactive Video Learning System for IIUM. *Academic Journal of Nawroz University*, 11(2), 23-29.
- [130] 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).
- [131] Zangana, H. M. (2024). Exploring Blockchain-Based Timestamping Tools: A Comprehensive Review. *Redefining Security With Cyber AI*, 92-110.
- [132] Zangana, H. M. (2024). Exploring the Landscape of Website Vulnerability Scanners: A Comprehensive Review and Comparative Analysis. *Redefining Security With Cyber AI*, 111-129.

- [133] Zangana, H. M. CHALLENGES AND ISSUES of MANET.
- [134] 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.
- [135] 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.
- [136] 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.
- [137] 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).
- [138] 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.
- [139] Zangana, H. M., & Omar, M. (2020). Threats, Attacks, and Mitigations of Smartphone Security. *Academic Journal of Nawroz University*, 9(4), 324-332.
- [140] Zangana, H. M., & Omar, M. (2020). Threats, Attacks, and Mitigations of Smartphone Security. *Academic Journal of Nawroz University*, 9(4), 324-332.
- [141] 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.
- [142] 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.
- [143] 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.
- [144] 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.
- [145] 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. *Sistemas: Jurnal Sistem Informasi*, 13(4), 1501-1509.
- [146] 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.
- [147] 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.
- [148] 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.
- [149] 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).
- [150] 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/tjab.v8.i1.2024.54618>
- [152] 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.
- [153] 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.

- [154] 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.
- [155] 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.
- [156] Zangana, H. M., Tawfiq, N. E., & Omar, M. (2020). Advantages and Challenges of E-Government in Turkey.
- [157] Zangana¹, H. M., Tawfiq, N. E., & Omar, M. (2020). Advantages and Challenges of E-Government in Turkey.
- [158] 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.
- [159] Zhou, S., Ali, A., Al-Fuqaha, A., Omar, M., & Feng, L. (n.d.). Robust Risk-Sensitive Task Offloading for
- [160] Edge-Enabled Industrial Internet of Things. *IEEE Transactions on Consumer Electronics*