Available on: http://gjetr.ep-journals.org/ E-ISSN: 3051-3782, P-ISSN: 3051-3774

Global Journal of Engineering and Technology Review

Volume: 02 Issue: 07 July 2026

The Imperative of Robust AI Governance: Addressing Risks and Ensuring Ethical Deployment

Rebet Jones
Kennesaw State University

Published Date: July 15, 2026 **Article DOI : 10.65150/EP-gjetr/V2E7/2026-05**

ABSTRACT: The rapid evolution of artificial intelligence (AI) has brought unprecedented opportunities and challenges. As AI systems become more integrated into critical aspects of society, the need for robust governance frameworks that address the ethical, safety, and fairness concerns become increasingly urgent. This paper explores the landscape of AI governance, identifying key challenges and proposing strategies for effective oversight. Through a detailed analysis of existing governance frameworks and a discussion of the core principles necessary for responsible AI deployment, this paper contributes to the ongoing discourse on how to harness AI's potential while mitigating its risks.

KEYWORDS: AI governance, ethical AI, AI risks, transparency, accountability, fairness

1. INTRODUCTION

Artificial Intelligence (AI) has rapidly advanced over the past decade, becoming a transformative force across various sectors, including healthcare, finance, transportation, and more. As AI technologies become more autonomous and pervasive, they bring with them not only opportunities but also significant risks. These risks include unintended consequences, biases in decision-making, and the erosion of human oversight in critical areas. The integration of AI into society has sparked a debate on how to govern these technologies effectively. Without appropriate governance frameworks, AI systems may exacerbate existing inequalities, lead to harmful outcomes, and erode public trust in technology. Therefore, there is a pressing need to develop and implement robust AI governance mechanisms that ensure these technologies are used responsibly and ethically.

This paper examines the current state of AI governance, focusing on the challenges and opportunities associated with developing frameworks that address the ethical and safety concerns surrounding AI. By analyzing existing governance models and proposing new strategies, this paper aims to contribute to the development of effective policies and practices for AI governance.

2. LITERATURE REVIEW

The literature on AI governance is extensive and varied, reflecting the complexity of the issues involved. Key themes in the literature include the ethical implications of AI, the need for transparency and accountability, and the challenges of regulating rapidly evolving technologies.

Ethical Implications: One of the central concerns in AI governance is the ethical implications of AI systems. Scholars have argued that AI technologies must be designed and deployed in a way that respects human rights, promotes fairness, and avoids harm. The concept of "ethical AI" has gained traction, with various frameworks proposed to guide the ethical development of AI technologies (Floridi et al., 2018; Mittelstadt et al., 2016).

Transparency and Accountability: Another critical theme in the literature is the need for transparency and accountability in AI systems. AI decision-making processes are often opaque, making it difficult to understand how decisions are made and who is responsible for the outcomes. This lack of transparency can lead to a lack of trust in AI systems and hinder their adoption (Doshi-Velez & Kim, 2017).

Regulation and Governance: The literature also highlights the challenges of regulating AI. AI technologies are evolving rapidly, and traditional regulatory approaches may not be sufficient to address the unique challenges posed by AI. There is a growing consensus that new governance models are needed, models that are flexible, adaptive, and capable of addressing the global nature of AI development (Cath, 2018; Gasser & Almeida, 2017).

3. METHODOLOGY

This research employs a qualitative approach, drawing on a review of existing literature, case studies, and expert interviews to explore the current state of AI governance. The analysis is focused on identifying the core principles that should underpin effective AI governance frameworks and examining how these principles are applied in practice.

Literature Review: The literature review involved a systematic search of academic databases for articles, reports, and books on AI governance. Key themes and trends were identified through a thematic analysis of the literature.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Case Studies: The research includes an analysis of several case studies where AI governance frameworks have been implemented. These case studies provide insights into the challenges and successes of different governance models.
Expert Interviews: To gain further insights into the practical aspects of AI governance, interviews were conducted with experts in AI ethics, policy, and law. These interviews provided valuable perspectives on the challenges of implementing governance frameworks and the factors that contribute to their success.

4. ANALYSIS

The analysis focuses on the core principles of AI governance transparency, accountability, fairness, and safety and examines how these principles are applied in existing governance frameworks.
Transparency: Transparency is a fundamental principle of AI governance. It involves making the decision-making processes of AI systems understandable and accessible to stakeholders. In practice, transparency can be challenging to achieve due to the complexity of AI algorithms and the proprietary nature of many AI systems. However, some governance frameworks have successfully implemented transparency measures, such as requiring AI developers to provide detailed documentation of their algorithms and decision-making processes.
Accountability: Accountability is closely related to transparency and involves ensuring that there are clear lines of responsibility for the actions of AI systems. This principle is particularly important in high-stakes environments, such as healthcare and criminal justice, where the consequences of AI decisions can be significant. Effective governance frameworks establish mechanisms for holding AI developers and operators accountable for the outcomes of their systems.
Fairness: Ensuring that AI systems are fair and do not perpetuate existing biases is another critical aspect of AI governance. This requires careful consideration of the data used to train AI models and ongoing monitoring to detect and mitigate any biases that may emerge. Some governance frameworks have introduced fairness audits and bias testing as part of the AI development process.
Safety: Safety is paramount in AI governance, particularly in applications where AI systems have the potential to cause harm. Governance frameworks must include rigorous testing and validation processes to ensure that AI systems are safe to use. This includes implementing fail-safe mechanisms and ensuring that AI systems can be overridden by human operators if necessary.

5. DISCUSSION

The analysis highlights the challenges and opportunities associated with AI governance. One of the main challenges is balancing the need for regulation with the need to foster innovation. Overly restrictive governance frameworks may stifle innovation and slow the adoption of AI technologies. On the other hand, insufficient regulation may lead to harmful outcomes and erode public trust in AI.
Another challenge is the global nature of AI development. AI technologies are developed and deployed across different countries and regions, each with its own legal and regulatory frameworks. This makes it difficult to establish a unified approach to AI governance. However, international cooperation and collaboration are essential for developing effective governance frameworks that can address the global nature of AI.
Despite these challenges, there are also significant opportunities for innovation in AI governance. New technologies, such as blockchain, could be used to enhance transparency and accountability in AI systems. Additionally, the development of new governance models, such as co-regulation and self-regulation, offers the potential to create more flexible and adaptive governance frameworks.

6. CONCLUSION

The governance of AI is a complex and rapidly evolving field. As AI technologies become more integrated into society, the need for robust governance frameworks that address the ethical, safety, and fairness concerns becomes increasingly urgent. This paper has explored the current state of AI governance, identified key challenges, and proposed strategies for effective oversight. By building on the core principles of transparency, accountability, fairness, and safety, we can develop governance frameworks that maximize the benefits of AI while minimizing its risks.
Future research should focus on developing new governance models that are flexible, adaptive, and capable of addressing the global nature of AI development. Additionally, there is a need for ongoing research into the ethical implications of AI and the development of new tools and techniques for ensuring the transparency and accountability of AI systems.

REFERENCES

1) V. Vitianingsih, D. Firmansyah, A. L. Maukar, S. Kacung, and H. M. Zangana, Recommendation System for Determining the Best Banner Supplier Using Profile Matching and TOPSIS Methods, Intensif, vol. 8, no. 2, pp. 246-262, Aug. 2024.
2) M. Basharat and M. Omar, 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, 2024.
3) H. M. Zangana, "A New Skin Color Based Face Detection Algorithm by Combining Three Color Model Algorithms," IOSR Journal of Computer Engineering, vol. 17, pp. 06-125, 2015.
4) M. Basharat and M. Omar, Harnessing GPT-2 for Feature Extraction in Malware Detection: A Novel Approach to Cybersecurity, Land Forces Academy Review, vol. 29, no. 1, pp. 74-84, 2024.
5) R. Abbasi, A. K. Bashir, A. Mateen, F. Amin, Y. Ge, and M. Omar, Efficient Security and Privacy of Lossless Secure Communication for Sensor-based Urban Cities, IEEE Sensors Journal, vol. 2023.
6) N. Ahmed, K. Mohammadani, A. K. Bashir, M. Omar, A. Jones, and F. Hassan, Secure and Reliable Routing in the Internet of Vehicles Network: AODV-RL with BHA Attack Defense, CMES-Computer Modeling in Engineering & Sciences, vol. 139, no. 1, 2024.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

7) H. M. Zangana, "A new algorithm for shape detection," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 19, no. 3, pp. 71-76, 2017.
8) Ahmed, H. Rasheed, A. K. Bashir, and M. Omar, Millimeter-wave Channel Modeling in a VANETs Using Coding Techniques, PeerJ Computer Science, vol. 9, p. e1374, 2023.
9) Arulappan, G. Raja, A. K. Bashir, A. Mahanti, and M. Omar, ZTMP: Zero Touch Management Provisioning Algorithm for the On-boarding of Cloud-native Virtual Network Functions, Mobile Networks and Applications, pp. 1-13, 2023.
10) N. Alturki, A. Altamimi, M. Umer, O. Saidani, A. Alshardan, S. Alsubai, M. Omar, and I. Ashraf, Improving Prediction of Chronic Kidney Disease Using KNN Imputed SMOTE Features and TrioNet Model, CMES-Computer Modeling in Engineering & Sciences, vol. 139, no. 3, 2024.
11) H. M. Zangana, "Library Data Quality Maturity (IIUM as a Case Study)," IOSR-JCE, vol. 29, Mar. 2017.
12) S. Al Harthi, M. Y. Al Balushi, A. H. Al Badi, J. Al Karaki, and M. Omar, Metaverse Adoption in UAE Higher Education: A Hybrid SEM-ANN Approach, in 98 Mohammad Daradkeh, Boshra Aldhanhani, Amjad Gawanmeh, Shadi Atalla and Sami Miniaoui. Applied Research Approaches to Technology, Healthcare, and Business, IGI Global.
13) M. Ayub, X. Li, K. Mahmood, S. Shamshad, M. A. Saleem, and M. Omar, Secure Consumer-centric Demand Response Management in Resilient Smart Grid as Industry 5.0 Application with Blockchain-based Authentication, IEEE Transactions on Consumer Electronics, 2023.
14) H. M. Zangana, "Watermarking System Using LSB," IOSR Journal of Computer Engineering, vol. 19, no. 3, pp. 75-79, 2017.
15) M. Al Kinoon, M. Omar, M. Mohaisen, and D. Mohaisen, 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, Springer International Publishing, pp. 171-183, 2021.
16) O. I. Al-Sanjary, A. A. Ahmed, H. M. Zangana, M. Ali, S. Aldulaimi, and M. Alkawaz, An Investigation of the Characteristics and Performance of Hybrid Routing Protocol in (MANET), International Journal of Engineering & Technology, vol. 7, no. 4.22, pp. 49-54, 2018.
17) H. M. Zangana, "Design an information management system for a pharmacy," International Journal of Advanced Research in Computer and Communication Engineering, vol. 7, no. 10, 2018.
18) H. M. Zangana, "Developing Data Warehouse for Student Information System (IIUM as a Case Study)," International Organization of Scientific Research, vol. 20, no. 1, pp. 09-14, 2018.
19) [19] O. I. Al-Sanjary, A. A. Ahmed, A. A. B. Jaharadak, M. A. Ali, and H. M. Zangana, Detection Clone an Object Movement Using an Optical Flow Approach, in 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), pp. 388-394, 2018.
20) M. Basharat and M. Omar, SecuGuard: Leveraging Pattern-exploiting Training in Language Models for Advanced Software Vulnerability Detection, International Journal of Mathematics and Computer in Engineering, 2024.
21) M. Banisakher, M. Omar, and W. Clare, Critical Infrastructure Perspectives on the Role of Government in Cybersecurity, Journal of Computer Sciences and Applications, vol. 7, no. 1, pp. 37-42, 2019.
22) H. M. Zangana, "Implementing a System for Recognizing Optical Characters," 2018.
23) H. M. Zangana, "Issues of Data Management in the Library: A Case Study," 2019.
24) D. N. Burrell, C. Nobles, K. Richardson, J. B. Wright, A. J. Jones, D. Springs, and K. Brown-Jackson, Allison Huff, in Applied Research Approaches to Technology, Healthcare, and Business, IGI Global, 2023.
25) M. Banisakher, D. Mohammed, and M. Omar, A Cloud-Based Computing Architecture Model of Post-Disaster Management System, International Journal of Simulation--Systems, Science & Technology, vol. 19, no. 5, 2018.
26) H. M. Zangana, "ITD Data Quality Maturity (A Case Study)," International Journal Of Engineering And Computer Science, vol. 8, no. 10, 2019.
27) M. Banisakher, M. Omar, S. Hong, and J. Adams, A Human-centric Approach to Data Fusion in Post-Disaster Management, Journal of Business Management and Science, vol. 8, no. 1, pp. 12-20, 2020.
28) H. M. Zangana, "Mobile Device Integration in IIUM Service," International Journal, vol. 8, no. 5, 2020.
29) J. N. Al-Karaki, M. Omar, A. Gawanmeh, and A. Jones, 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, 2023.
30) L. Davis, M. Dawson, and M. Omar, 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, IGI Global, pp. 483-509, 2016.
31) H. M. Zangana, "The Global Financial Crisis from an Islamic Point Of View," Qubahan Academic Journal, vol. 1, no. 2, pp. 55-59, 2021.
32) H. M. Zangana, "Creating a Community-Based Disaster Management System," Academic Journal of Nawroz University, vol. 11, no. 4, pp. 234-244, 2022.
33) M. Dawson, A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism, in New Threats and Countermeasures in Digital Crime and Cyber Terrorism, IGI Global, pp. 1-7, 2015.
34) D. N. Burrell, C. Nobles, A. Cusak, M. Omar, and L. Gillesania, Cybercrime and the Nature of Insider Threat Complexities in Healthcare and Biotechnology Engineering Organizations, Journal of Crime and Criminal Behavior, vol. 2, no. 2, pp. 131-144, 2022.
35) M. Dawson, I. Al Saeed, J. Wright, and M. Omar, Technology enhanced learning with open source software for scientists and engineers, in INTED2013 Proceedings, IATED, 2013, pp. 5583 5589.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

36) H. M. Zangana, "Implementing New Interactive Video Learning System for IIUM," Academic Journal of Nawroz University, vol. 11, no. 2, pp. 23-29, 2022.
37) M. Dawson, L. Davis, and M. Omar, Developing learning objects for engineering and science fields: using technology to test system usability and interface design, Int. J. Smart Technol. Learn., vol. 1, no. 2, pp. 140 161, 2019.
38) H. M. Zangana, "Improving The Web Services for Remittance Company: Express Remit as a Case Study," Academic Journal of Nawroz University (AJNU), vol. 11, no. 3, 2022.
39) M. Dawson, M. Eltayeb, and M. Omar, Security solutions for hyperconnectivity and the Internet of things. IGI Global, 2016.
40) H. M. Zangana, "Exploring Blockchain-Based Timestamping Tools: A Comprehensive Review," Redefining Security With Cyber AI, pp. 92-110, 2024.
41) M. Dawson, M. Omar, and J. Abramson, Understanding the methods behind cyber terrorism, in Encyclopedia of Information Science and Technology, Third Edition, IGI Global, 2015, pp. 1539 1549.
42) H. M. Zangana, "Exploring the Landscape of Website Vulnerability Scanners: A Comprehensive Review and Comparative Analysis," Redefining Security With Cyber AI, pp. 111-129, 2024.
43) H. M. Zangana, "CHALLENGES AND ISSUES of MANET," 2024.
44) M. Dawson, M. Omar, J. Abramson, and D. Bessette, Information security in diverse computing environments. Academic Press, 2014.
45) H. M. Zangana and A. M. Abdulazeez, "Developed Clustering Algorithms for Engineering Applications: A Review," International Journal of Informatics, Information System and Computer Engineering (INJIISCOM), vol. 4, no. 2, pp. 147-169, 2023.
46) M. Dawson, M. Omar, J. Abramson, and D. Bessette, The future of national and international security on the internet, in Information security in diverse computing environments, IGI Global, 2014, pp. 149 178.
47) H. M. Zangana and I. F. Al-Shaikhli, "A new algorithm for human face detection using skin color tone," IOSR Journal of Computer Engineering, vol. 11, no. 6, pp. 31-38, 2013.
48) M. Dawson, M. Omar, J. Abramson, B. Leonard, and D. Bessette, Battlefield cyberspace: Exploitation of hyperconnectivity and Internet of Things, in Developing Next-Generation Countermeasures for Homeland Security Threat Prevention, IGI Global, 2017, pp. 204 235.
49) H. M. Zangana and F. M. Mustafa, "From Classical to Deep Learning: A Systematic Review of Image Denoising Techniques," Jurnal Ilmiah Computer Science, vol. 3, no. 1, pp. 50-65, 2024.
50) M. Dawson, J. Wright, and M. Omar, Mobile devices: The case for cyber security hardened systems, in New Threats and Countermeasures in Digital Crime and Cyber Terrorism, IGI Global, 2015, pp. 8 29.
51) H. M. Zangana and F. M. Mustafa, "Review of Hybrid Denoising Approaches in Face Recognition: Bridging Wavelet Transform and Deep Learning," The Indonesian Journal of Computer Science, vol. 13, no. 4, 2024.
52) Dayoub and M. Omar, Advancing IoT security posture K-Means clustering for malware detection, in Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology, IGI Global, 2024, pp. 221 239.
53) H. Dong, J. Wu, A. K. Bashir, Q. Pan, M. Omar, and A. Al-Dulaimi, Privacy-preserving EEG signal analysis with electrode attention for depression diagnosis: Joint FHE and CNN approach, in GLOBECOM 2023-2023 IEEE Global Communications Conference, IEEE, 2023, pp. 4265 4270.
54) D. Fawzi and M. Omar, New insights to database security: An effective and integrated approach to applying access control mechanisms and cryptographic concepts in Microsoft access environments. Academic Press, n.d.
55) S. Gholami, Can pruning make large language models more efficient? in Redefining Security With Cyber AI, IGI Global, 2024, pp. 1 14.
56) H. M. Zangana and F. M. Mustafa, "Surveying the Landscape: A Comprehensive Review of Object Detection Algorithms and Advancements," Jurnal Ilmiah Computer Science, vol. 3, no. 1, pp. 1-15, 2024.
57) S. Gholami, Do generative large language models need billions of parameters? in Redefining Security With Cyber AI, IGI Global, 2024, pp. 37 55.
58) H. M. Zangana and M. Omar, "Threats, Attacks, and Mitigations of Smartphone Security," Academic Journal of Nawroz University, vol. 9, no. 4, pp. 324-332, 2020.
59) S. Gholami and M. Omar, Does synthetic data make large language models more efficient? arXiv preprint arXiv:2310.07830, 2023.
60) H. M. Zangana and S. R. Zeebaree, "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), vol. 5, no. 1, pp. 11-30, 2024.
61) S. Gholami and M. Omar, Can a student large language model perform as well as its teacher? in Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology, IGI Global, 2024, pp. 122 139.
62) Y. A. Hamza and M. D. Omar, Cloud computing security: Abuse and nefarious use of cloud computing, Int. J. Comput. Eng. Res., vol. 3, no. 6, pp. 22 27, 2013.
63) H. M. Zangana, I. F. Al-Shaikhli, and Y. I. Graha, "The Ethical Dilemma of Software Piracy: An Inquiry from an Islamic Perspective," Creative Communication and Innovative Technology Journal, vol. 7, no. 1, pp. 59-76, 2013.
64) J. Huff, D. N. Burrell, C. Nobles, K. Richardson, J. B. Wright, S. L. Burton, A. J. Jones, D. Springs, M. Omar, and K. L. Brown-Jackson, Management practices for mitigating cybersecurity threats to biotechnology companies, laboratories, and healthcare research organizations, in Applied Research Approaches to Technology, Healthcare, and Business, IGI Global, 2023, pp. 1 12.
65) Jabbari, H. Khan, S. Duraibi, I. Budhiraja, S. Gupta, and M. Omar, Energy maximization for wireless powered communication enabled IoT devices with NOMA underlaying solar powered UAV using federated reinforcement learning for 6G networks, IEEE Trans. Consum. Electron., 2024.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Corresponding Author: Rebet Jones

66) H. M. Zangana, S. M. S. Bazeed, N. Y. Ali, and D. T. Abdullah, "Navigating Project Change: A Comprehensive Review of Change Management Strategies and Practices," Indonesian Journal of Education and Social Sciences, vol. 3, no. 2, pp. 166-179, 2024.
67) Jones and M. Omar, Harnessing the efficiency of reformers to detect software vulnerabilities, in 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), IEEE, 2023, pp. 2259 2264.
68) H. M. Zangana, Y. I. Graha, and I. F. Al-Shaikhli, "Blogging: A New Platform For Spreading Rumors!," Creative Communication and Innovative Technology Journal, vol. 9, no. 1, pp. 71-76, 2024.
69) Jones and M. Omar, Optimized decision trees to detect IoT malware, in 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), IEEE, 2023, pp. 1761 1765.
70) H. M. Zangana, A. Khalid Mohammed, and S. R. Zeebaree, "Systematic Review of Decentralized and Collaborative Computing Models in Cloud Architectures for Distributed Edge Computing," Sistemasi: Jurnal Sistem Informasi, vol. 13, no. 4, pp. 1501-1509, 2024.
71) Jones and M. Omar, Codesentry: Revolutionizing real-time software vulnerability detection with optimized GPT framework, Land Forces Acad. Rev., vol. 29, no. 1, pp. 98 107, 2024.
72) H. M. Zangana, A. K. Mohammed, and F. M. Mustafa, "Advancements and Applications of Convolutional Neural Networks in Image Analysis: A Comprehensive Review," Jurnal Ilmiah Computer Science, vol. 3, no. 1, pp. 16-29, 2024.
73) M. Jones and M. Omar, 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), IEEE, 2023, pp. 511 516.
74) H. M. Zangana, A. K. Mohammed, and F. M. Mustafa, "Advancements in Edge Detection Techniques for Image Enhancement: A Comprehensive Review," International Journal of Artificial Intelligence & Robotics (IJAIR), vol. 6, no. 1, pp. 29-39, 2024.
75) M. Jones and M. Omar, Measuring the impact of global health emergencies on self-disclosure using language models, in 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), IEEE, 2023, pp. 1806 1810.
76) H. M. Zangana, A. K. Mohammed, A. B. Sallow, and Z. B. Sallow, "Cybernetic Deception: Unraveling the Layers of Email Phishing Threats," International Journal of Research and Applied Technology (INJURATECH), vol. 4, no. 1, pp. 35-47, 2024.
77) M. Jones and M. Omar, Studying the effects of social media content on kids' safety and well-being, in 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), IEEE, 2023, pp. 1876 1879.
78) R. Jones and M. Omar, "Detecting IoT Malware with Knowledge Distillation Technique," in 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), pp. 131-135, IEEE, 2023.
79) H. M. Zangana, A. K. Mohammed, Z. B. Sallow, and F. M. Mustafa, "Exploring Image Representation and Color Spaces in Computer Vision: A Comprehensive Review," The Indonesian Journal of Computer Science, vol. 13, no. 3, 2024.
80) R. Jones and M. Omar, "Codeguard: Utilizing Advanced Pattern Recognition in Language Models for Software Vulnerability Analysis," Land Forces Academy Review, vol. 29, no. 1, pp. 108-118, 2024.
81) R. Jones and M. Omar, "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), vol. 5, no. 2, pp. 178-191, 2024.
82) R. Jones, M. Omar, and D. Mohammed, "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, 2023.
83) R. Jones, M. Omar, D. Mohammed, and C. Nobles, "IoT Malware Detection with GPT Models," in 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), pp. 1749-1752, IEEE, 2023.
84) R. Jones, M. Omar, D. Mohammed, C. Nobles, and M. Dawson, "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, 2023.
85) W. Jun, M. S. Iqbal, R. Abbasi, M. Omar, and C. Huiqin, "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), vol. 20, no. 1, pp. 1-16, IGI Global, 2024.
86) S. A. Khan, M. H. Alkawaz, and H. M. Zangana, "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, 2019.
87) V. A. Kumar, S. Surapaneni, D. Pavitra, R. Venkatesan, M. Omar, and A. K. Bashir, "An Internet of Medical Things-Based Mental Disorder Prediction System Using EEG Sensor and Big Data Mining," Journal of Circuits, Systems and Computers, vol. 2450197, World Scientific Publishing Company, 2024.
88) H. Majeed, "Watermarking Image Depending on Mojette Transform for Hiding Information," International Journal Of Computer Sciences And Engineering, vol. 8, pp. 8-12, 2020.
89) Mohammed and M. Omar, "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, 2024.
90) M. Omar, "Insider Threats: Detecting and Controlling Malicious Insiders," in New Threats and Countermeasures in Digital Crime and Cyber Terrorism, pp. 162-172, IGI Global, 2015.
91) Mohammed, M. Omar, and V. Nguyen, "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, 2017.
92) M. Omar, Smartphone Security: Defending Android-based Smartphone Against Emerging Malware Attacks (Doctoral dissertation, Colorado Technical University), 2012.
93) Mohammed, M. Omar, and V. Nguyen, "Wireless Sensor Network Security: Approaches to Detecting and Avoiding Wormhole Attacks," Journal of Research in Business, Economics and Management, vol. 10, no. 2, pp. 1860-1864, 2018.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

94) M. Omar, "New Insights into Database Security: An Effective and Integrated Approach for Applying Access Control Mechanisms and Cryptographic Concepts in Microsoft Access Environments," 2021.
95) V. Nguyen, D. Mohammed, M. Omar, and M. Banisakher, "The Effects of the FCC Net Neutrality Repeal on Security and Privacy," International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), vol. 2, no. 2, pp. 21-29, IGI Global, 2018.
96) V. Nguyen, M. Omar, D. Mohammed, and P. Dean, "Net Neutrality Around the Globe: A Survey," in 2020 3rd International Conference on Information and Computer Technologies (ICICT), pp. 480-488, IEEE, 2020.
97) M. Omar, "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, 2022.
98) V. Nguyen, M. Omar, and D. Mohammed, "A Security Framework for Enhancing User Experience," International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), vol. 1, no. 1, pp. 19-28, IGI Global, 2017.
99) M. Omar and H. M. Zangana, "Redefining Security With Cyber AI," IGI Global, 2024. https://doi.org/10.4018/979-8-3693-6517-5
100) N. Tiwari, M. Omar, and Y. Ghadi, "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, 2023.
101) M. Omar, "A World of Cyber Attacks (A Survey)," 2019.
102) N. Tiwari, Y. Ghadi, and M. Omar, "Analysis of Ultrasound Images in Kidney Failure Diagnosis Using Deep Learning," in Transformational Interventions for Business, Technology, and Healthcare, pp. 45-74, IGI Global, 2023.
103) M. Omar, Machine Learning for Cybersecurity: Innovative Deep Learning Solutions, Springer Brief, 2022. https://link.springer.com/book/978303115
104) X. Xu, J. Wu, A. K. Bashir, and M. Omar, "Machine Learning and Zero Knowledge Empowered Trustworthy Bitcoin Mixing for Next-G Consumer Electronics Payment," IEEE Transactions on Consumer Electronics, 2024.
105) M. Omar, "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, 2015.
106) H. Zhang, J. Wu, Q. Pan, A. K. Bashir, and M. Omar, "Toward Byzantine-Robust Distributed Learning for Sentiment Classification on Social Media Platform," IEEE Transactions on Computational Social Systems, 2024.
107) M. Omar, "Malware Anomaly Detection Using Local Outlier Factor Technique," in Machine Learning for Cybersecurity: Innovative Deep Learning Solutions, pp. 37-48, Springer International Publishing Cham, 2022.
108) M. Omar, "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, 2023.
109) M. Omar, "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, 2024.
110) M. Omar, "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, 2024.
111) M. Omar, Defending Cyber Systems through Reverse Engineering of Criminal Malware, Springer Brief, [n.d.]. https://link.springer.com/book/9783031116278
112) M. Omar, Latina Davis Morgan State University 1700 E Cold Spring Ln. Baltimore, MD 21251, USA E-mail: latinaedavis@ hotmail.com, [n.d.].
113) M. Omar, Machine Learning for Cybersecurity, [n.d.].
114) M. Omar and D. Burrell, "From Text to Threats: A Language Model Approach to Software Vulnerability Detection," International Journal of Mathematics and Computer in Engineering, 2023.
115) M. Omar and D. N. Burrell, "Organizational Dynamics and Bias in Artificial Intelligence (AI) Recruitment Algorithms," in Evolution of Cross-Sector Cyber Intelligent Markets, pp. 269-290, IGI Global, 2024.
116) M. Omar and M. Dawson, "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, 2013.
117) M. Omar and D. Mohaisen, "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, 2022.
118) M. Omar and S. Shiaeles, "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
119) M. Omar and G. Sukthankar, "Text-Defend: Detecting Adversarial Examples Using Local Outlier Factor," in 2023 IEEE 17th International Conference on Semantic Computing (ICSC), pp. 118-122, IEEE, 2023.
120) M. Omar et al., "Committee Members," Journal of Physics: Conference Series, vol. 2711, p. 011001, 2024.
121) S. Zhou, A. Ali, A. Al-Fuqaha, M. Omar, and L. Feng, Robust Risk-Sensitive Task Offloading for Edge-Enabled Industrial Internet of Things, IEEE Transactions on Consumer Electronics, 2024.
122) M. Omar, S. Choi, D. Nyang, and D. Mohaisen, "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, 2022.
123) M. Omar, S. Choi, D. Nyang, and D. Mohaisen, "Robust Natural Language Processing: Recent Advances, Challenges, and Future Directions," IEEE Access, vol. 10, pp. 86038-86056, 2022.
124) M. Omar, L. B. Gouveia, J. Al-Karaki, and D. Mohammed, "Reverse-Engineering Malware," in Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security, pp. 194-217, IGI Global, 2022.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Corresponding Author: Rebet Jones

125) M. A. Saleem et al., "Provably Secure Conditional-Privacy Access Control Protocol for Intelligent Customers-Centric Communication in VANET," IEEE Transactions on Consumer Electronics, 2023.
126) H. M. Zangana, M. Omar, and N. Y. Ali, "Harnessing Artificial Intelligence in Modern Marketing: Strategies, Benefits, and Challenges," Business, Accounting and Management Journal (BAMJ), vol. 02, no. 02, pp. 70 82, 2024.
127) M. Omar, R. Jones, D. N. Burrell, M. Dawson, C. Nobles, and D. Mohammed, "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, 2023.
128) R. Rajesh et al., "Threat Detection and Mitigation for Tactile Internet Driven Consumer IoT-Healthcare System," IEEE Transactions on Consumer Electronics, 2024.
129) M. Omar, D. Mohammed, and V. Nguyen, "Defending Against Malicious Insiders: A Conceptual Framework for Predicting, Detecting, and Deterring Malicious Insiders," International Journal of Business Process Integration and Management, vol. 8, no. 2, pp. 114-119, 2017.
130) Y. Peng et al., "An Intelligent Resource Allocation Strategy with Slicing and Auction for Private Edge Cloud Systems," Future Generation Computer Systems, vol. 160, pp. 879-889, North-Holland, 2024.
131) M. Omar, D. Mohammed, V. Nguyen, M. Dawson, and M. Banisakher, "Android Application Security," in Research Anthology on Securing Mobile Technologies and Applications, pp. 610-625, IGI Global, 2021.
132) K. T. Pauu, Q. Pan, J. Wu, A. K. Bashir, and M. Omar, "IRS-Aided Federated Learning with Dynamic Differential Privacy for UAVs in Emergency Response," IEEE Internet of Things Magazine, vol. 7, no. 4, pp. 108-115, IEEE, 2024.
133) Y. Sun, T. Xu, A. K. Bashir, J. Liu, and M. Omar, "BcIIS: Blockchain-Based Intelligent Identification Scheme of Massive IoT Devices," in GLOBECOM 2023-2023 IEEE Global Communications Conference, pp. 1277-1282, IEEE, 2023.
134) H. M. Zangana, Z. B. Sallow, M. H. Alkawaz, and M. Omar, "Unveiling the Collective Wisdom: A Review of Swarm Intelligence in Problem Solving and Optimization," Inform: Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi, vol. 9, no. 2, pp. 101-110, 2024.
135) M. Umer et al., "Heart Failure Patients Monitoring Using IoT-Based Remote Monitoring System," Scientific Reports, vol. 13, no. 1, p. 19213, 2023.
136) H. M. Zangana, M. Omar, J. N. Al-Karaki, and D. Mohammed, "Comprehensive Review and Analysis of Network Firewall Rule Analyzers: Enhancing Security Posture and Efficiency," Redefining Security With Cyber AI, pp. 15-36, 2024.
137) S. Zhou, A. Ali, A. Al-Fuqaha, M. Omar, and L. Feng, "Robust Risk-Sensitive Task Offloading for Edge-Enabled Industrial Internet of Things," IEEE Transactions on Consumer Electronics, 2024.
138) Y. Tao, J. Wu, Q. Pan, A. K. Bashir, and M. Omar, "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, 2024.
139) J. Wright, M. E. Dawson Jr, and M. Omar, "Cyber Security and Mobile Threats: The Need for Antivirus Applications for Smartphones," Journal of Information Systems Technology and Planning, vol. 5, no. 14, pp. 40-60, 2012.
140) H. Zhang, J. Wu, Q. Pan, A. K. Bashir, and M. Omar, Toward Byzantine-Robust Distributed Learning for Sentiment Classification on Social Media Platform, IEEE Transactions on Computational Social Systems, 2024.
141) H. M. Zangana, M. A. Mirza, S. Wani, X. Cao, and M. Omar, Hybrid Vision Transformer for Brain and Lung Tumor Detection: A Multi-Modal Approach Using MRI (BraTS) and CT (LUNA16) Datasets , Buletin Ilmiah Sarjana Teknik Elektro, vol. 7, no. 4, pp. 1069 1081, Feb. 2026.
142) H. M. Zangana, Ed., Defense in Depth: Modern Cybersecurity Strategies and Evolving Threats. Wiley, 2025. doi: 10.1002/9781394340750.
143) H. Zangana and M. Omar, Eds., Securing Large Language Models Against Emerging Threats. IGI Global Scientific Publishing, 2026. doi: 10.4018/979-8-3373-7133-7.
144) A. Mohammed and H. Zangana, Eds., Intelligent Construction Monitoring Systems: Real-Time Safety, Environmental Prediction, and Risk Management. IGI Global Scientific Publishing, 2026. doi: 10.4018/979-8-3373-9245-5.
145) H. M. Zangana and M. A. Sulaiman, "Explainable Transformer Models for Early Prediction of Chronic Diseases Using Longitudinal Electronic Health Records (EHRs)," EAI Endorsed Transactions on AI and Robotics, vol. 5, 2026. doi: 10.4108/airo.11517.
146) Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608. https://arxiv.org/abs/1702.08608
147) Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Corresponding Author: Rebet Jones