International Journal of Research in Engineering, Science and Management
Volume 8, Issue 2, February 2025
https://www.ijresm.com | ISSN (Online): 2581-5792

A Comprehensive System Review of Large Language Models Utilization in Cybersecurity

Hermano Jorge De Queiroz[1], Marwan Omar[2*]
[1]*Lindsey Wilson College, United States of America*
[2]*ITM, Illinois Institute of Technology, United States of America*

***Abstract*: Large Language Models (LLMs) have emerged as powerful tools in the realm of cybersecurity, enabling advancements in areas such as threat detection, vulnerability assessment, and security automation. This review provides an in-depth analysis of LLM applications in cybersecurity, highlighting both the opportunities and challenges associated with their deployment. The paper addresses issues related to bias, interpretability, and adversarial robustness while proposing future research directions. Drawing on a comprehensive set of references, the review underscores the transformative potential of LLMs in enhancing cybersecurity practices.**

***Keywords*: LLMs, Cybersecurity, Optimization, Deep Learning.**

1. Introduction

As cyber threats continue to evolve in complexity and frequency, the need for advanced cybersecurity measures becomes increasingly critical. Large Language Models (LLMs), with their capabilities in natural language processing (NLP), offer promising solutions for various cybersecurity challenges. LLMs such as GPT-3, BERT, and others have demonstrated their ability to process and analyze large volumes of textual data, making them suitable for applications in threat detection, incident response, and more [1]-[15]. This review paper explores the current state of LLM utilization in cybersecurity, examining their applications, challenges, and future research directions. By integrating insights from recent studies, this paper aims to provide a comprehensive overview of how LLMs are transforming the cybersecurity landscape [16]-[50].

LLMs have shown significant potential in enhancing threat detection and incident response capabilities. By analyzing security logs, network traffic, and other textual data, LLMs can identify patterns indicative of cyber threats. For instance, LLMs can be trained to detect phishing attempts by analyzing email content, identifying suspicious language patterns, and flagging potential threats for further investigation [51]-[75]. Additionally, LLMs can support incident response by generating automated recommendations for mitigating detected threats, thereby reducing the time required for human analysts to respond to security incidents [76]-[100].

2. Research Method

Table 1
Applications of LLMs in cybersecurity
This table summarizes the different applications of LLMs in cybersecurity, along with specific examples and references.

Application Area	Description	Example	Reference
Threat Detection and Incident Response	Use of LLMs to identify and respond to security threats by analyzing text data.	Phishing detection through email content analysis.	Ahmed et al., 2024
Vulnerability Assessment	Analysis of codebases and documentation to identify security flaws.	Identification of software vulnerabilities and patch suggestions.	Jones & Omar, 2023
Security Automation and Orchestration	Automation of routine cybersecurity tasks such as alert triaging.	SOAR platforms integrating LLMs for automated alert responses.	Abbasi et al., 2023

Table 2
Challenges of LLMs in cybersecurity
This table outlines the main challenges associated with deploying LLMs in cybersecurity, with descriptions and examples.

Challenge	Description	Example	Reference
Bias and Fairness	Risk of biased decision-making due to skewed training data.	Overemphasis on certain threats while underestimating others.	Zangana et al., 2024
Interpretability and Transparency	Difficulty in understanding how LLMs arrive at certain decisions.	Black-box nature of LLMs making it hard to validate outputs.	Omar & Burrell, 2024
Adversarial Attacks and Robustness	Vulnerability to inputs that manipulate LLMs into making errors.	False positives or negatives due to adversarial attacks.	Gholami & Omar, 2023

Table 3
Future research directions
This table presents potential research directions to address the challenges of LLMs in cybersecurity.

Research Direction	Description	Example	Reference
Enhancing Model Robustness	Developing methods to protect LLMs against adversarial attacks.	Training with adversarial examples and model pruning.	Gholami, 2024
Improving Interpretability	Making LLMs more transparent and understandable for analysts.	Integration of explainable AI techniques into LLMs.	Omar & Sukthankar, 2023
Ethical Considerations and Bias Mitigation	Ensuring that LLMs operate fairly and ethically.	Using diverse datasets and bias correction techniques.	Burrell et al., 2022

A. Security Automation and Orchestration

LLMs are increasingly being integrated into Security Orchestration, Automation, and Response (SOAR) platforms, where they play a key role in automating routine cybersecurity tasks. These tasks include triaging alerts, generating security reports, and correlating data from various sources to provide a comprehensive view of an organization's security posture (Abbasi et al., 2023). The automation provided by LLMs can

*Corresponding author: drmarwan.omar@gmail.com

significantly reduce the workload on security teams, allowing them to focus on more complex tasks, such as threat hunting and incident investigation [101]-[140].

Description:

- *Step 1*: Data Collection - Security logs, network traffic, and other textual data are collected.
- *Step 2*: Data Processing - The collected data is processed and normalized for analysis.
- *Step 3*: LLM Analysis - The data is fed into an LLM, which analyzes the text for patterns and anomalies.
- *Step 4*: Threat Detection - The LLM identifies potential threats based on detected patterns.
- *Step 5*: Automated Response - The LLM generates automated recommendations or triggers an incident response.

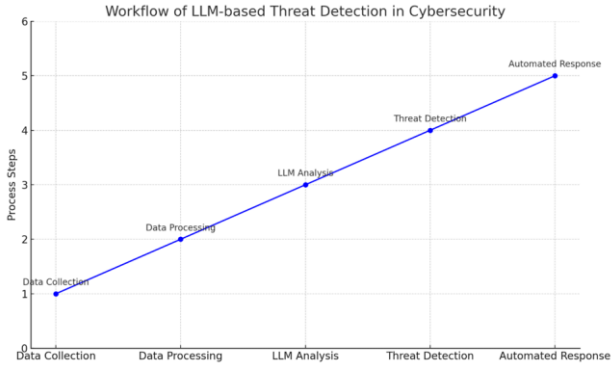

Fig. 1. Workflow of LLM-based threat detection in cybersecurity this figure could illustrate the workflow of how LLMs are used in threat detection, from data collection to threat identification and response

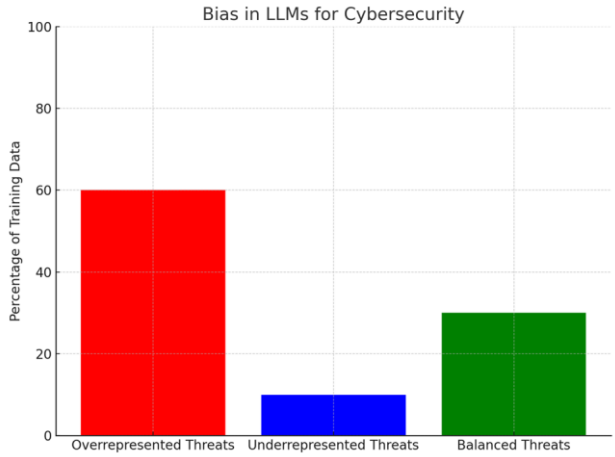

Fig. 2. Bias in LLMs for cybersecurity this figure could depict how bias can influence the outputs of LLMs in cybersecurity, leading to skewed threat detection

Description:

- *Illustration of Training Data* - Shows a pie chart or bar graph of the training data composition, highlighting the overrepresentation of certain threat types.
- *LLM Output* - Demonstrates how the bias in training data leads to overemphasis on specific threats while underestimating others.
- *Impact on Security Decisions* - Illustrates the potential consequences of biased outputs on security decision-making.

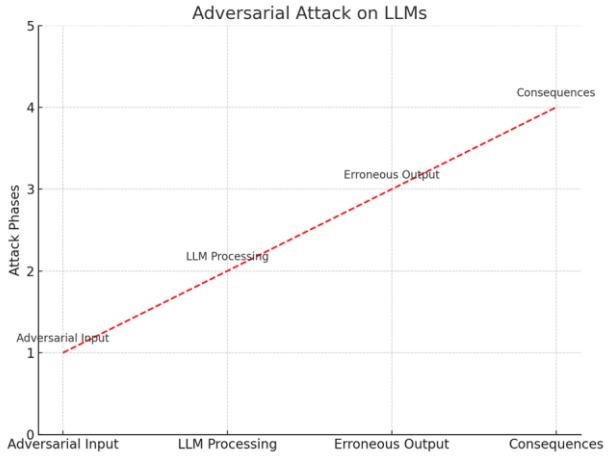

Fig. 3. This figure could illustrate how an adversarial attack can manipulate an LLM into making incorrect decisions

Description:

- *Adversarial Input* - Shows how an attacker crafts a malicious input designed to deceive the LLM.
- *LLM Processing* - Illustrates the LLM analyzing the input without recognizing the adversarial nature.
- *Erroneous Output* - Depicts the LLM generating a false positive or negative based on the manipulated input.
- *Consequences* - Highlights the potential security risks stemming from the erroneous output.

3. Challenges and Limitations

A. *Bias and Fairness*

One of the major challenges associated with the deployment of LLMs in cybersecurity is the potential for bias in the model's outputs. Bias in training data can lead to skewed threat assessments or disproportionate responses, undermining the reliability of cybersecurity measures. For example, if an LLM is trained on data that predominantly represents certain types of threats, it may overemphasize those threats while underestimating others. This issue is further complicated by the inherent biases present in cybersecurity data, such as geographic or linguistic biases, which can affect the performance of LLMs.

B. *Interpretability and Transparency*

LLMs are often criticized for their lack of interpretability, making it difficult to understand how they arrive at certain decisions. This "black-box" nature poses significant challenges in cybersecurity, where transparency is crucial for understanding threats and ensuring compliance [140]. Security analysts need to comprehend why an LLM has flagged a particular event as suspicious or recommended a specific course of action. Without this understanding, validating the model's outputs and making informed decisions becomes challenging [141].

C. Adversarial Attacks and Robustness

LLMs themselves can be susceptible to adversarial attacks, where inputs are intentionally manipulated to deceive the model. This vulnerability raises concerns about the robustness of LLMs in real-world cybersecurity scenarios, where they could become targets for sophisticated attacks. Adversaries could exploit weaknesses in the LLM to bypass detection or manipulate the model's outputs, creating false positives or negatives. Ensuring that LLMs are resilient to such attacks is a critical challenge that must be addressed to maintain their reliability in cybersecurity applications.

4. Future Research Directions

A. Enhancing Model Robustness

Future research should focus on developing methods to enhance the robustness of LLMs against adversarial attacks. This could involve training models with adversarial examples or using techniques like model pruning to reduce vulnerabilities. Additionally, research could explore the development of hybrid models that combine the strengths of LLMs with other machine learning techniques to improve overall robustness and resilience [125]. Such approaches could help mitigate the risks associated with adversarial attacks and ensure that LLMs remain effective in dynamic cybersecurity environments.

B. Improving Interpretability

Advancements in explainable AI (XAI) can contribute to making LLMs more interpretable, which is essential for their widespread adoption in cybersecurity. Research should explore how to integrate XAI techniques into LLMs without compromising their performance. For example, methods such as attention mechanisms or layer-wise relevance propagation could be employed to provide insights into the decision-making processes of LLMs, allowing security analysts to better understand and trust the model's outputs [123]. Additionally, developing visualization tools that present the inner workings of LLMs in an accessible manner could further enhance their interpretability (Omar & Burrell, 2024).

C. Ethical Considerations and Bias Mitigation

Addressing ethical concerns, such as bias and fairness, is critical for the responsible use of LLMs in cybersecurity. Future research should focus on developing bias mitigation strategies during both the training and deployment phases of LLMs. This could involve using diverse and representative datasets for training, as well as implementing post-hoc bias correction techniques to ensure that LLMs make fair and equitable decisions. Furthermore, ethical frameworks should be established to guide the deployment of LLMs in cybersecurity, ensuring that they are used in a manner that respects privacy, fairness, and human rights [124].

5. Conclusion

The integration of Large Language Models into cybersecurity presents a promising avenue for enhancing threat detection, automating responses, and improving overall security posture. However, significant challenges remain, particularly in terms of model interpretability, robustness, and ethical considerations. By addressing these challenges through focused research, LLMs can become a cornerstone of modern cybersecurity practices, providing organizations with powerful tools to combat evolving cyber threats. The future of cybersecurity lies in the responsible and ethical use of LLMs, which can unlock new possibilities for securing digital environments.

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. Peer J Computer Science, 9, e1374. Peer J 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.
[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.
[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.
[76] Omar, M. (n.d.). Latina Davis Morgan State University 1700 E Cold Spring Ln. Baltimore, MD 21251, USA.
[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.
[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). Implementing a System for Recognizing Optical Characters.
[109] Zangana, H. M. (2019). Issues of Data Management in the Library: A Case Study.
[110] Zangana, H. M. (2019). ITD Data Quality Maturity (A Case Study). International Journal Of Engineering And Computer Science, 8(10).
[111] Zangana, H. M. (2020). Mobile Device Integration in IIUM Service. International Journal, 8(5).
[112] Zangana, H. M. (2021). The Global Finical Crisis from an Islamic Point Of View. Qubahan Academic Journal, 1(2), 55-59.
[113] Zangana, H. M. (2022). Creating a Community-Based Disaster Management System. Academic Journal of Nawroz University, 11(4), 234-244.
[114] Zangana, H. M. (2022). Implementing New Interactive Video Learning System for IIUM. Academic Journal of Nawroz University, 11(2), 23-29.
[115] 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).
[116] Zangana, H. M. (2024). Exploring Blockchain-Based Timestamping Tools: A Comprehensive Review. Redefining Security with Cyber AI, 92-110.
[117] Zangana, H. M. (2024). Exploring the Landscape of Website Vulnerability Scanners: A Comprehensive Review and Comparative Analysis. Redefining Security with Cyber AI, 111-129.
[118] Zangana, H. M. Challenges and Issues of MANET.
[119] 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.
[120] 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.
[121] Zangana, H. M., & Mustafa, F. M. (2024). From Classical to Deep Learning: A Systematic Review of Image Denoising Techniques. Journal Ilmiah Computer Science, 3(1), 50-65.
[122] 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).
[123] 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.
[124] Zangana, H. M., & Omar, M. (2020). Threats, Attacks, and Mitigations of Smartphone Security. Academic Journal of Nawroz University, 9(4), 324-332.
[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., & 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.
[127] 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.
[128] 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.
[129] 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.
[130] 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.
[131] 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.
[132] 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.
[133] 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.
[134] 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).
[135] 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.
[136] 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.
[137] 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.
[138] Zangana, H. M., Tawfiq, N. E., & Omar, M. (2020). Advantages and Challenges of E-Government in Turkey.
[139] 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.
[140] 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