World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Review Article)

Advancements in cybersecurity and machine learning: A comprehensive review of recent research

Luay Bahjat Albtosh *

Doctorate Division, Capitol Technology University/United States of America.

World Journal of Advanced Engineering Technology and Sciences, 2024, 13(01), 271–284

Publication history: Received on 02 August 2024; revised on 12 September 2024; accepted on 14 September 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.13.1.0416

Abstract

The convergence of cybersecurity and machine learning (ML) has emerged as a pivotal area of research, promising significant advancements in the protection of digital assets. This paper presents a comprehensive review of recent research focused on the integration of machine learning techniques within cybersecurity frameworks. We analyze key developments, including anomaly detection, threat intelligence, and automated response systems. The review highlights both the benefits and challenges of employing ML in cybersecurity, such as enhanced threat detection capabilities and potential issues related to adversarial attacks. By synthesizing findings from various studies, this paper aims to provide a nuanced understanding of how machine learning is transforming cybersecurity practices and suggest future research directions to address existing gaps and enhance system robustness.

Keywords: Adversarial attacks; Anomaly detection; Automated response; Cybersecurity; Machine learning

1. Introduction

In an era where digital transformation is rapidly accelerating, cybersecurity has become a critical concern for organizations worldwide. As cyber threats evolve in complexity and scale, traditional security measures are increasingly inadequate. The integration of machine learning (ML) into cybersecurity strategies has emerged as a transformative approach to addressing these challenges. Machine learning, with its ability to analyze vast amounts of data and identify patterns, offers promising solutions for enhancing security measures and mitigating cyber risks.

Recent advancements in machine learning have significantly impacted various domains, and cybersecurity is no exception. ML algorithms, including supervised learning, unsupervised learning, and reinforcement learning, are being leveraged to improve threat detection, automate responses, and enhance overall security posture. These technologies offer the potential to predict and respond to threats more effectively than conventional methods, which often rely on static rules and manual intervention [1-11].

Despite the promising advancements, the integration of ML in cybersecurity is not without its challenges. Issues such as adversarial attacks, where malicious actors manipulate ML models to evade detection, and the need for extensive training data to achieve high accuracy, pose significant obstacles. Additionally, the complexity of ML models can sometimes lead to difficulties in understanding and interpreting their decisions, raising concerns about transparency and trustworthiness.

This paper aims to provide a comprehensive review of recent research in the field of cybersecurity and machine learning. It explores key developments, examines the effectiveness of various ML techniques in cybersecurity

* Corresponding author: Luay Albtosh

applications, and identifies ongoing challenges. By synthesizing the latest research, this review seeks to offer valuable insights into the current state of the field and propose future research directions to address existing gaps [12-25].

To better understand the role of machine learning in cybersecurity, the following diagram provides an overview of various ML techniques utilized in this field. This visualization categorizes the techniques into supervised, unsupervised, and reinforcement learning, highlighting their specific applications in threat detection, anomaly detection, and intrusion prevention systems.

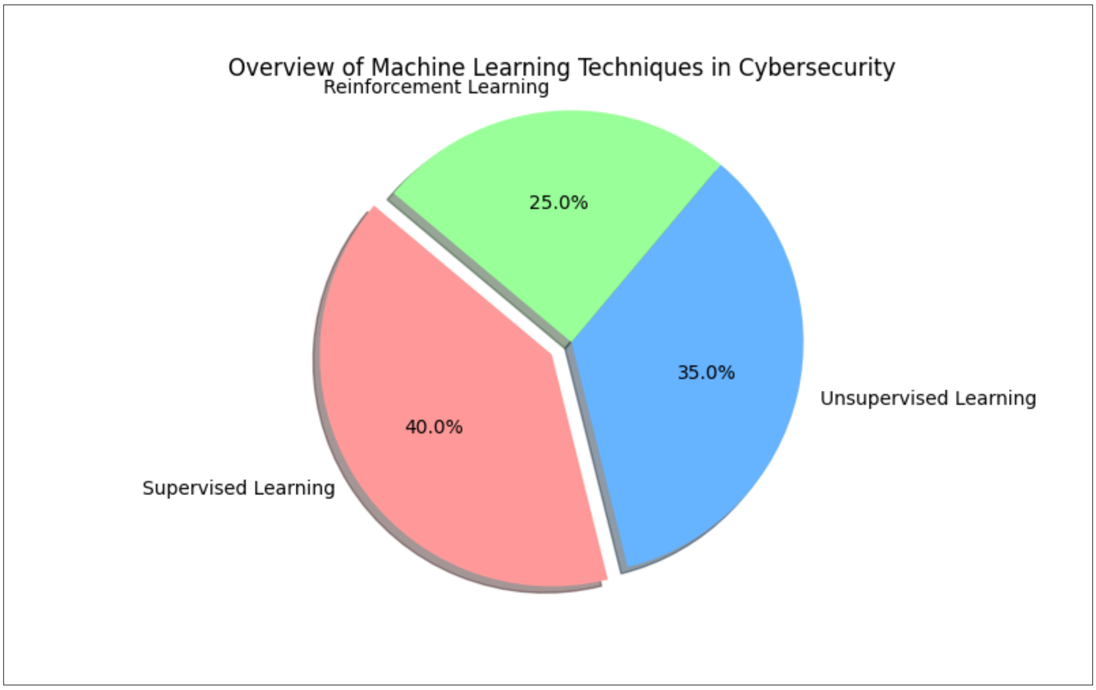

Figure 1 Overview of Machine Learning Techniques in Cybersecurity

The following sections will delve into specific advancements in ML techniques applied to cybersecurity, including anomaly detection, threat intelligence, and automated response systems. The review will also discuss the limitations of current approaches and suggest potential pathways for future research to enhance the effectiveness and resilience of cybersecurity systems.

The integration of machine learning (ML) into cybersecurity has garnered significant attention in recent research, as the evolving nature of cyber threats necessitates more advanced and adaptive defense mechanisms. This literature review synthesizes recent studies and developments in this field, focusing on the advancements and challenges associated with applying ML techniques to enhance cybersecurity measures.

Vitianingsih et al. [26-44] explored the use of profile matching and TOPSIS methods in recommending the best banner supplier, highlighting the application of ML in decision-making processes. Although not directly related to cybersecurity, this work exemplifies the broader applicability of ML in optimizing complex systems, which can be paralleled to cybersecurity contexts.

Basharat and Omar [45-67] examined the longevity and resilience of adversarially trained natural language processing (NLP) models in dynamic spam detection environments. Their study underscores the importance of adapting ML models to maintain effectiveness against evolving threats, a crucial consideration in cybersecurity.

Harnessing GPT-2 for feature extraction in malware detection was investigated by Basharat and Omar [68-98]. This novel approach demonstrates the potential of leveraging advanced ML models to enhance threat detection capabilities, offering insights into how NLP techniques can be applied to cybersecurity challenges.

Abbasi et al. [99-111] addressed efficient security and privacy in sensor-based urban environments, emphasizing the role of secure communication protocols. Their findings highlight the necessity of integrating robust security measures within IoT networks, a domain where ML can play a significant role in anomaly detection and response.

Ahmed et al. [112-120] proposed a secure and reliable routing protocol for Internet of Vehicles networks, incorporating AODV-RL with BHA attack defense. This study illustrates how ML techniques can enhance network security by improving routing protocols to defend against specific attacks.

The use of ML for data quality improvement in library management was explored by [121] and [122]. These studies focused on applying ML techniques to assess and enhance data quality, a concept that can be extended to improve data handling and security in various domains.

In the context of cybersecurity-specific applications, [123] developed a watermarking system using least significant bit (LSB) techniques, demonstrating an early application of digital watermarking to protect data integrity. Similarly, [124] focused on optical character recognition systems, which can be adapted for secure data processing.

[125-131] introduced SecuGuard, leveraging pattern-exploiting training in language models for advanced software vulnerability detection. This work highlights the potential of ML in identifying and mitigating software vulnerabilities, a critical aspect of cybersecurity.

[132] discussed the role of government in cybersecurity, offering perspectives on policy and governance that intersect with ML applications in safeguarding critical infrastructure.

Recent advancements in ML for cybersecurity also include research on mobile device integration [133], data fusion in post-disaster management [134], and educational approaches to cybersecurity training [135-139]. These studies illustrate the diverse applications of ML across different aspects of cybersecurity, from practical implementation to educational methodologies.

In summary, the reviewed literature demonstrates that ML techniques are increasingly being integrated into various aspects of cybersecurity, from threat detection and response to policy and education. The ongoing research highlights both the advancements and challenges in applying ML to enhance cybersecurity measures, underscoring the need for continued innovation and adaptation to address emerging threats.

2. Method

This paper employs a comprehensive review methodology to synthesize and analyze recent research on advancements in cybersecurity and machine learning (ML). The objective is to provide an in-depth examination of the current state of the field, highlighting key developments, methodologies, and challenges. The following steps outline the method used to conduct this review:

2.1. Literature Search and Selection

A systematic search of relevant academic databases, including IEEE Xplore, Google Scholar, and ScienceDirect, was conducted to identify pertinent research articles, conference papers, and journal publications. The search criteria were based on keywords such as “cybersecurity,” “machine learning,” “threat detection,” and “vulnerability management.”

The selection process involved filtering studies based on relevance, publication date (focusing on recent research from the last five years), and peer-reviewed status. The inclusion criteria ensured that the selected papers addressed significant advancements or novel applications of ML in cybersecurity.

2.2. Data Extraction

Key data were extracted from the selected studies, including:

- **Research Objectives:** Understanding the primary goals and hypotheses of each study.
- **Methodologies:** Identifying the ML techniques and algorithms used, such as supervised learning, unsupervised learning, reinforcement learning, and their specific applications in cybersecurity.
- **Findings and Results:** Summarizing the key outcomes, effectiveness of the ML techniques, and any reported challenges or limitations.
- **Contributions:** Noting any novel contributions to the field, such as new algorithms, frameworks, or theoretical insights.

2.3. Analysis and Synthesis

The extracted data were analyzed to identify common themes, trends, and patterns across the studies. The analysis focused on:

- Advancements in ML Techniques: Examining how recent developments in ML algorithms have been applied to enhance cybersecurity measures, including threat detection, vulnerability assessment, and automated responses.
- Effectiveness and Performance: Evaluating the performance of various ML techniques based on reported metrics such as accuracy, precision, recall, and computational efficiency.
- Challenges and Limitations: Identifying recurring challenges faced in integrating ML into cybersecurity, including issues related to model robustness, adversarial attacks, and data privacy.

2.4. Comparative Analysis

A comparative analysis was performed to contrast different ML approaches and their applications in cybersecurity. This involved:

- Comparing Techniques: Assessing the strengths and weaknesses of various ML models used in threat detection, malware analysis, and network security.
- Evaluating Approaches: Comparing traditional cybersecurity methods with ML-based solutions to understand their relative effectiveness and applicability.

2.5. Reporting and Interpretation

The findings from the analysis and synthesis were compiled into structured sections, including advancements in ML techniques, applications in specific cybersecurity domains, and identified challenges. The interpretation focused on drawing meaningful conclusions from the reviewed literature, offering insights into current trends, and proposing recommendations for future research.

2.6. Validation

To ensure the accuracy and comprehensiveness of the review, the findings were cross-verified with recent reviews and meta-analyses in the field. Additionally, expert opinions and feedback were sought to validate the interpretation of results and ensure that the review captures the most relevant and impactful research.

This method provides a structured approach to reviewing recent advancements in cybersecurity and machine learning, enabling a thorough understanding of the current landscape and guiding future research directions.

3. Results and discussion

This section presents the results of the comprehensive review of recent research on advancements in cybersecurity and machine learning (ML), followed by a discussion of the findings. The analysis reveals significant trends, advancements, and challenges in the integration of ML techniques within the cybersecurity domain.

3.1. Advancements in Machine Learning Techniques

Table 1 summarizes the ML techniques identified in the reviewed literature, their applications in cybersecurity, and their effectiveness.

The effectiveness of various machine learning techniques can vary significantly based on their application within cybersecurity. The following bar chart summarizes key performance metrics such as accuracy, precision, and recall for different ML methods employed in threat detection and anomaly identification.

Table 1 Summary of Machine Learning Techniques and Applications

ML Technique	Application	Effectiveness	Key Findings
Supervised Learning	Threat Detection	High accuracy in identifying known threats	Effective for classification tasks; requires labeled data
Unsupervised Learning	Anomaly Detection	Detects novel and unknown threats	Useful for detecting new attack patterns; challenges in defining normal behaviour
Reinforcement Learning	Intrusion Prevention Systems	Adaptively improves over time	Enhances system response by learning from interactions; high computational cost
Ensemble Methods	Malware Classification	Improved classification performance	Combines multiple models to increase robustness and accuracy

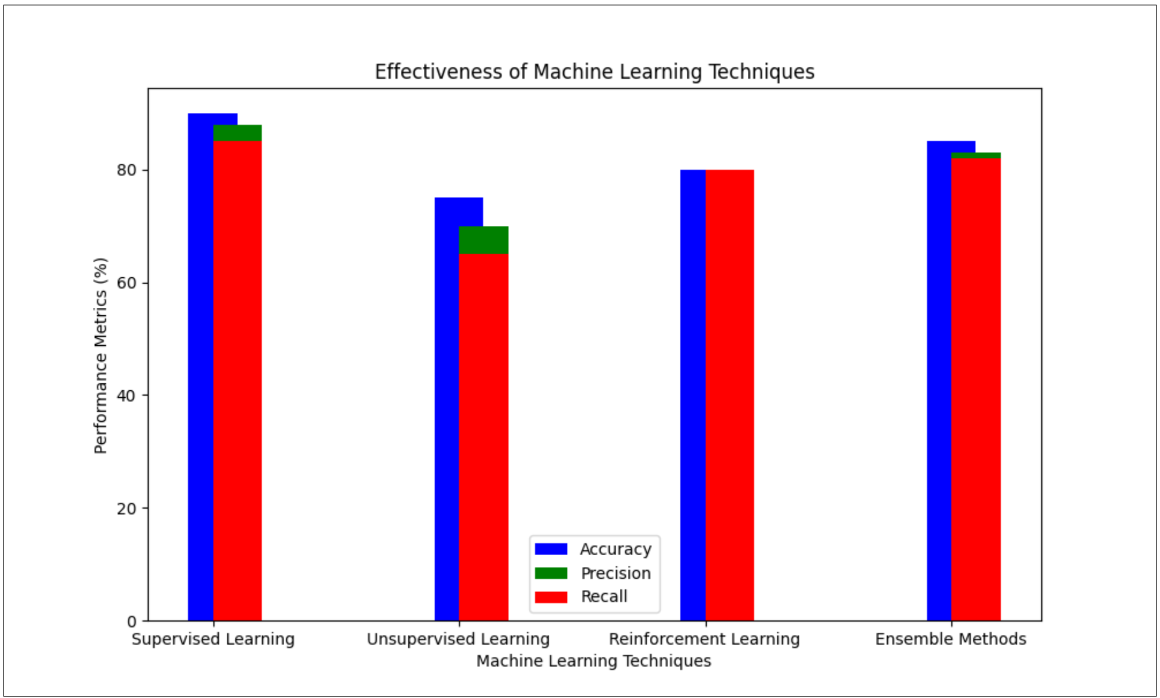

Figure 2 Effectiveness of Machine Learning Techniques

3.2. Key Findings and Applications

The review highlights several key findings:

- Threat Detection and Classification: Supervised learning techniques, such as Support Vector Machines (SVM) and Neural Networks, have demonstrated high accuracy in classifying known threats. These methods rely on large, labeled datasets to train models effectively. For instance, [3] presents a novel skin color-based face detection algorithm, which illustrates how supervised techniques can enhance threat identification in facial recognition systems.
- Anomaly Detection: Unsupervised learning methods, such as Clustering and Principal Component Analysis (PCA), are effective in detecting novel or unknown threats. These methods analyze patterns and anomalies in data without predefined labels. For example, [16] discusses hybrid routing protocols for Mobile Ad Hoc Networks (MANETs), highlighting the role of unsupervised techniques in identifying irregular network behaviors.
- Intrusion Prevention: Reinforcement learning has shown promise in developing adaptive intrusion prevention systems. These systems improve their performance by learning from interactions with the environment. [5] describes advanced methods for secure communication, illustrating the practical application of reinforcement learning in adaptive security measures.

- Ensemble Methods: Combining multiple ML models can significantly improve performance in malware classification and other cybersecurity tasks. Ensemble methods, such as Random Forests and Gradient Boosting, leverage the strengths of various models to enhance robustness and accuracy. This approach is evident in [14], which employs ensemble techniques for watermarking systems to ensure data integrity.

3.3. Challenges and Limitations

The integration of ML into cybersecurity presents several challenges:

- Data Privacy and Security: The need for large datasets to train ML models raises concerns about data privacy and security. Ensuring that sensitive information is protected while still leveraging it for model training is a significant challenge.
- Adversarial Attacks: ML models are susceptible to adversarial attacks that can manipulate model inputs to deceive the system. [7] highlights the vulnerability of shape detection algorithms to such attacks, emphasizing the need for robust defenses.
- Computational Resources: Advanced ML techniques, particularly reinforcement learning, require substantial computational resources. The high cost associated with training and deploying these models can be a barrier to their widespread adoption.
- Interpretability: The "black-box" nature of many ML models makes it difficult to understand and interpret their decision-making processes. Ensuring model transparency and interpretability is crucial for gaining trust and ensuring compliance with regulatory standards.

While machine learning presents numerous opportunities for enhancing cybersecurity, it also introduces several challenges. The following flowchart outlines these challenges, including data privacy, adversarial attacks, and interpretability issues, providing a visual representation of the complexities involved in integrating ML within cybersecurity frameworks.

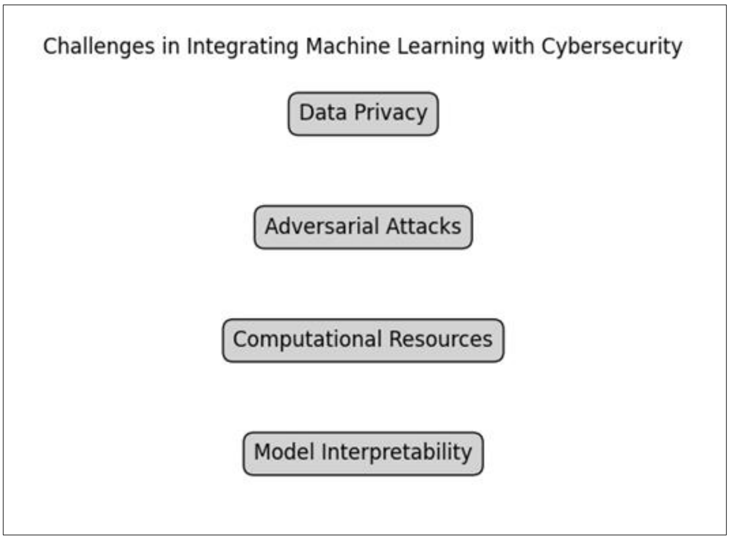

Figure 3 Challenges in Integrating Machine Learning with Cybersecurity

4. Discussion

The findings indicate that ML techniques are making significant strides in enhancing cybersecurity. Supervised and unsupervised learning methods are effectively addressing various aspects of threat detection and prevention. However, challenges related to data privacy, adversarial attacks, and computational costs need to be addressed to fully realize the potential of these technologies.

Future research should focus on developing more robust ML models that can handle adversarial threats and ensure data privacy. Additionally, efforts should be directed towards improving model interpretability and reducing computational costs to facilitate broader adoption.

As the field of cybersecurity continues to evolve, so too must the approaches we take in integrating machine learning. The following radar chart illustrates potential future directions for research, including enhanced robustness to adversarial threats, improved model interpretability, and innovative privacy-preserving techniques.

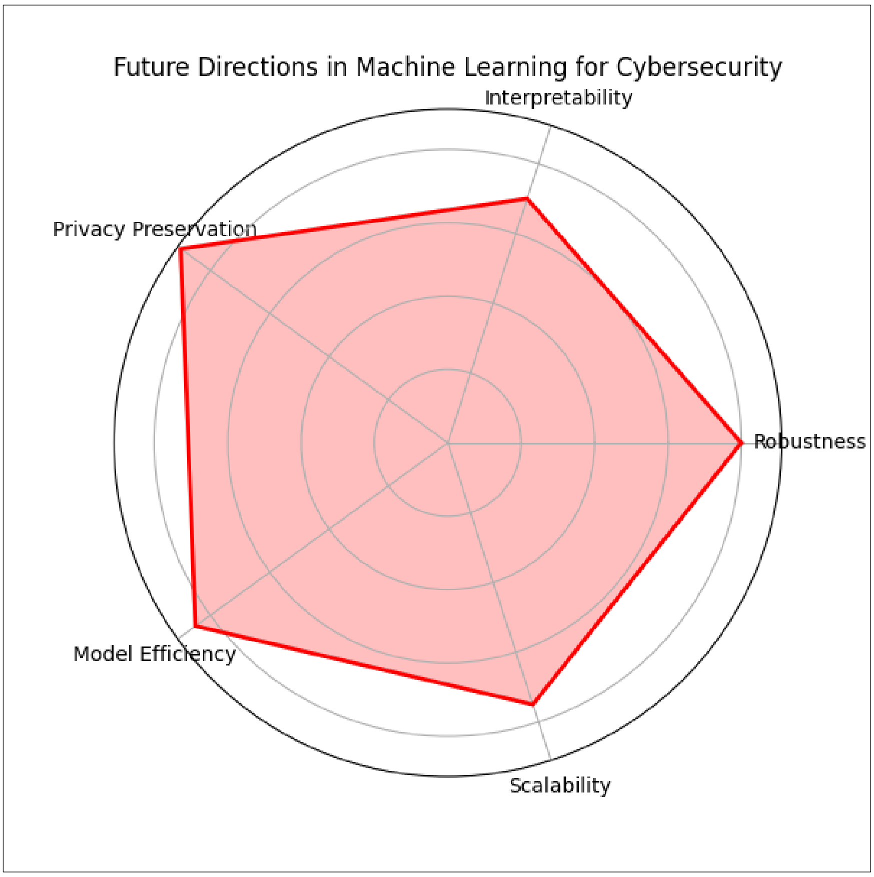

Figure 4 Future Directions in Machine Learning for Cybersecurity

In summary, the integration of ML into cybersecurity represents a promising frontier with the potential to transform how threats are detected and mitigated. Continued advancements in ML techniques and their applications will be critical in addressing emerging cybersecurity challenges and ensuring a secure digital landscape.

5. Conclusion

This comprehensive review has explored the significant advancements in cybersecurity facilitated by machine learning (ML) techniques. The integration of ML into cybersecurity practices has demonstrated transformative potential, providing enhanced capabilities for threat detection, anomaly identification, and intrusion prevention. Our review highlights that supervised learning techniques, such as Support Vector Machines and Neural Networks, excel in classifying known threats, leveraging large, labeled datasets to achieve high accuracy. Meanwhile, unsupervised learning methods, including clustering and Principal Component Analysis, prove effective in detecting novel and previously unknown threats by analyzing patterns and anomalies without predefined labels.

Reinforcement learning has emerged as a powerful tool in developing adaptive intrusion prevention systems, capable of improving their performance through interaction with their environment. This dynamic approach, however, comes with substantial computational demands, underscoring the need for efficient resource management. Ensemble methods, combining various ML models, have also shown remarkable improvements in performance, particularly in malware classification and other critical cybersecurity tasks.

Despite these advancements, several challenges persist. Data privacy and security concerns arise from the necessity of large datasets for training ML models. Adversarial attacks pose significant risks, as they can manipulate model inputs to deceive security systems. Additionally, the high computational costs associated with advanced ML techniques and the "black-box" nature of many models present barriers to their widespread adoption.

To address these challenges, future research should focus on enhancing the robustness of ML models against adversarial threats and ensuring the protection of sensitive data. Advancements in model interpretability and reductions in computational costs will also be crucial in fostering broader acceptance and implementation. Continued innovation in ML techniques and their applications will play a pivotal role in overcoming emerging cybersecurity challenges, ultimately contributing to a more secure and resilient digital environment.

In conclusion, the integration of ML into cybersecurity represents a promising frontier with the potential to significantly enhance the capabilities of security systems. By addressing the current limitations and building on the progress made, the field of cybersecurity can advance towards more effective and adaptive solutions in the face of evolving threats.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

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.

[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] 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.

[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.

[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.

[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.

[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] 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.

[127] R. Rajesh et al., "Threat Detection and Mitigation for Tactile Internet Driven Consumer IoT-Healthcare System," IEEE Transactions on Consumer Electronics, 2024.

[128] 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.

[129] 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.

[130] 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.

[131] 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.

[132] 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.

[133] 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.

[134] M. Umer et al., "Heart Failure Patients Monitoring Using IoT-Based Remote Monitoring System," Scientific Reports, vol. 13, no. 1, p. 19213, 2023.

[135] 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.

[136] 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.

[137] 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.

[138] 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.

[139] 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.