The Indonesian Journal of Computer Science
www.ijcs.net
Volume 13, Issue 4, August 2024
https://doi.org/10.33022/ijcs.v13i4.4383

The Impact of AI on Secure Cloud Computing: Opportunities and Challenges

Rebet Jones
rjones@captechu.edu
Capitol Technology Univerity, United States of America

Article Information

Received : 27 Aug 2024
Revised : 30 Aug 2024
Accepted : 31 Aug 2024

Keywords

AI, Cloud Computing

Abstract

This paper explores the intersection of Artificial Intelligence (AI) and cloud computing, focusing on the security implications. As cloud computing becomes increasingly ubiquitous, the integration of AI presents both opportunities and challenges. This paper provides an in-depth analysis of how AI can enhance cloud security, the potential risks associated with AI deployment in the cloud, and the future landscape of AI-driven cloud security. Key topics include AI's role in threat detection, data protection, access management, and the challenges related to AI bias, interpretability, and adversarial attacks.

A. Introduction

Cloud computing has fundamentally transformed the way organizations manage, store, and process data, offering unprecedented scalability, flexibility, and cost-efficiency. By enabling businesses to access computing resources on-demand, cloud computing has facilitated the rapid deployment of applications and services across various industries. However, this widespread adoption has also introduced a new set of security challenges, as sensitive data and critical infrastructure are increasingly being hosted on third-party platforms. In this context, ensuring the security of cloud environments has become a top priority for organizations, particularly as cyber threats continue to evolve in complexity and frequency.

Artificial Intelligence (AI), with its advanced capabilities in data analysis, pattern recognition, and decision-making, has emerged as a powerful tool in addressing the security challenges associated with cloud computing. AI technologies, such as machine learning (ML) and deep learning, can process vast amounts of data in real-time, enabling the detection of complex threats and the automation of security responses. As a result, AI-driven security solutions are becoming integral to modern cloud environments, providing organizations with the ability to proactively defend against cyber attacks while maintaining compliance with regulatory requirements (Saleem et al., 2023).

One of the most significant opportunities presented by AI in cloud security is its potential to enhance threat detection and response. Traditional security systems often rely on rule-based methods that can struggle to keep pace with the dynamic nature of cyber threats. In contrast, AIdriven systems can continuously learn from new data, adapting to emerging threats and providing real-time insights into potential vulnerabilities. For example, machine learning algorithms can analyze network traffic, user behavior, and system logs to identify anomalies that may indicate a security breach. By automating these processes, AI not only improves the accuracy of threat detection but also reduces the time required to respond to incidents, thereby minimizing the potential impact of cyber attacks (Basharat & Omar, 2024).

In addition to threat detection, AI is playing a crucial role in enhancing data protection and privacy in cloud environments. As organizations store increasingly large volumes of sensitive information in the cloud, the risk of data breaches and unauthorized access has grown correspondingly. AI technologies can help mitigate these risks through advanced encryption techniques, automated data classification, and real-time monitoring of data access patterns. For instance, AI-driven encryption algorithms can dynamically adjust the level of encryption based on the sensitivity of the data, ensuring that critical information remains secure even if other security measures are compromised (Gholami & Omar, 2023). Moreover, AI can identify unusual access patterns that may indicate an insider threat or an external attack, allowing for immediate intervention before any significant damage is done.

Another key area where AI is making a substantial impact is in intelligent access management. Traditional access control systems often operate based on static rules and predefined user roles, which can be insufficient in today's fast-paced, cloud-based environments. AI can enhance these systems by continuously monitoring user behavior and adapting access controls in real-time based on dynamic risk assessments. This approach, often referred to as adaptive access

management, ensures that users are granted the appropriate level of access at any given time, based on their current behavior and the context of their activities. For example, if a user suddenly attempts to access sensitive data from an unusual location or device, the AI system can automatically flag the activity as suspicious and require additional authentication before granting access (Abbasi et al., 2023). This not only enhances security but also improves the user experience by reducing the need for manual intervention in access management processes.

Security automation and orchestration are also areas where AI is proving to be invaluable. Managing security in a cloud environment often involves coordinating multiple tools and processes, which can be both time-consuming and prone to error. AI-driven Security Orchestration, Automation, and Response (SOAR) platforms can integrate various security technologies, automating tasks such as vulnerability scanning, patch management, and compliance monitoring. By automating these routine tasks, AI allows security teams to focus on more complex issues that require human expertise, thereby increasing the overall efficiency and effectiveness of the organization's security posture (Jones & Omar, 2024).

However, the integration of AI into cloud security is not without its challenges. One of the most significant concerns is the potential for bias in AI models, which can arise from the data used to train these models. If the training data is not representative of the full spectrum of possible scenarios, the AI system may develop biases that could lead to unfair or inaccurate security decisions. For example, an AI system trained primarily on data from a specific industry or geographic region may not perform well in other contexts, potentially missing critical threats or generating false positives (Burrell et al., 2022). This issue is further complicated by the blackbox nature of many AI models, particularly those based on deep learning, which can make it difficult to understand how decisions are being made. This lack of transparency can be problematic in security contexts, where understanding the rationale behind decisions is crucial for trust and compliance (Omar & Burrell, 2024).

Another challenge associated with AI in cloud security is the risk of adversarial attacks. These attacks involve manipulating inputs to AI models in a way that causes the model to make incorrect predictions or classifications. In the context of cloud security, adversarial attacks could lead to false positives or negatives in threat detection, potentially allowing malicious activities to go undetected or causing unnecessary disruptions to legitimate activities (Omar & Mohaisen, 2022). Ensuring the robustness of AI models against such attacks is a critical area of ongoing research and development.

Finally, the scalability and complexity of integrating AI into cloud security must be carefully managed. Cloud environments are often large and distributed, with diverse workloads and user bases. Implementing AI-driven security solutions in such environments requires significant computational resources and careful coordination to ensure that the AI models perform effectively across all parts of the system. Additionally, as AI technologies continue to evolve, organizations must be prepared to adapt their security strategies and infrastructure to accommodate new developments, which can add to the operational complexity (Gholami & Omar, 2023).

In conclusion, while AI offers substantial opportunities for enhancing cloud

security, it also introduces new challenges that must be addressed to fully realize its potential. By leveraging AI's strengths in threat detection, data protection, access management, and security automation, organizations can build more resilient and secure cloud environments. However, to ensure the successful integration of AI into cloud security, it is essential to address issues related to bias, transparency, adversarial robustness, and scalability. The following sections of this paper will explore these opportunities and challenges in greater detail, providing insights into the future of AI-driven cloud security.

Table 1: Opportunities of AI in Secure Cloud Computing

Opportunity	Description	Reference
Enhanced Threat Detection and Response	AI processes large data volumes to detect threats and automate incident responses.	Saleem et al., 2023
Data Protection and Privacy	AI-driven encryption and data masking techniques to protect data.	Gholami & Omar, 2023
Intelligent Access Management	AI monitors user behavior for dynamic access control based on risk assessment.	Abbasi et al., 2023
Security Automation and Orchestration	AI automates security tasks such as vulnerability scanning and compliance monitoring.	Basharat & Omar, 2024

Table 2: Challenges of AI in Secure Cloud Computing

Challenge	Description	Reference
Bias and Fairness	Potential for biased AI models due to skewed training data, leading to unfair decisions.	Burrell et al., 2022
Interpretability and Transparency	Lack of transparency in AI models, making it hard to understand their decision-making process.	Omar & Burrell, 2024
Adversarial Attacks	Vulnerability of AI models to adversarial inputs, leading to false security decisions.	Omar & Mohaisen, 2022
Scalability and Complexity	Challenges in scaling AI models across large cloud environments and managing their complexity.	Jones & Omar, 2024

B. Opportunities of AI in Secure Cloud Computing

2.1 Enhanced Threat Detection and Response

AI's ability to process vast amounts of data in real-time enables it to detect threats more effectively than traditional methods. Machine learning algorithms can identify patterns and anomalies in network traffic, application behavior, and user activity, providing early warning signs of potential security incidents (Saleem et al., 2023). AI can also automate incident response, reducing the time to mitigate threats.

2.2 Data Protection and Privacy

AI-driven encryption techniques and data masking can enhance data protection in the cloud. AI can automatically classify sensitive data and apply appropriate security measures, ensuring that data is protected throughout its lifecycle (Gholami & Omar, 2023). Additionally, AI can monitor data access patterns to detect unauthorized access and prevent data breaches.

2.3 Intelligent Access Management

AI can improve access management by continuously monitoring user behavior and adapting access controls based on real-time risk assessments (Abbasi et al., 2023). This dynamic approach to access management helps to prevent unauthorized access and reduces the risk of insider threats.

Figures:

- AI-Driven Threat Detection Workflow in Cloud Computing: This figure illustrates the workflow involved in AI-driven threat detection within cloud environments.
- AI in Data Protection and Privacy: This figure shows the contribution of AI in different aspects of data protection and privacy.
- Challenges of AI in Cloud Security: This figure visualizes the impact of various challenges associated with AI in cloud security.

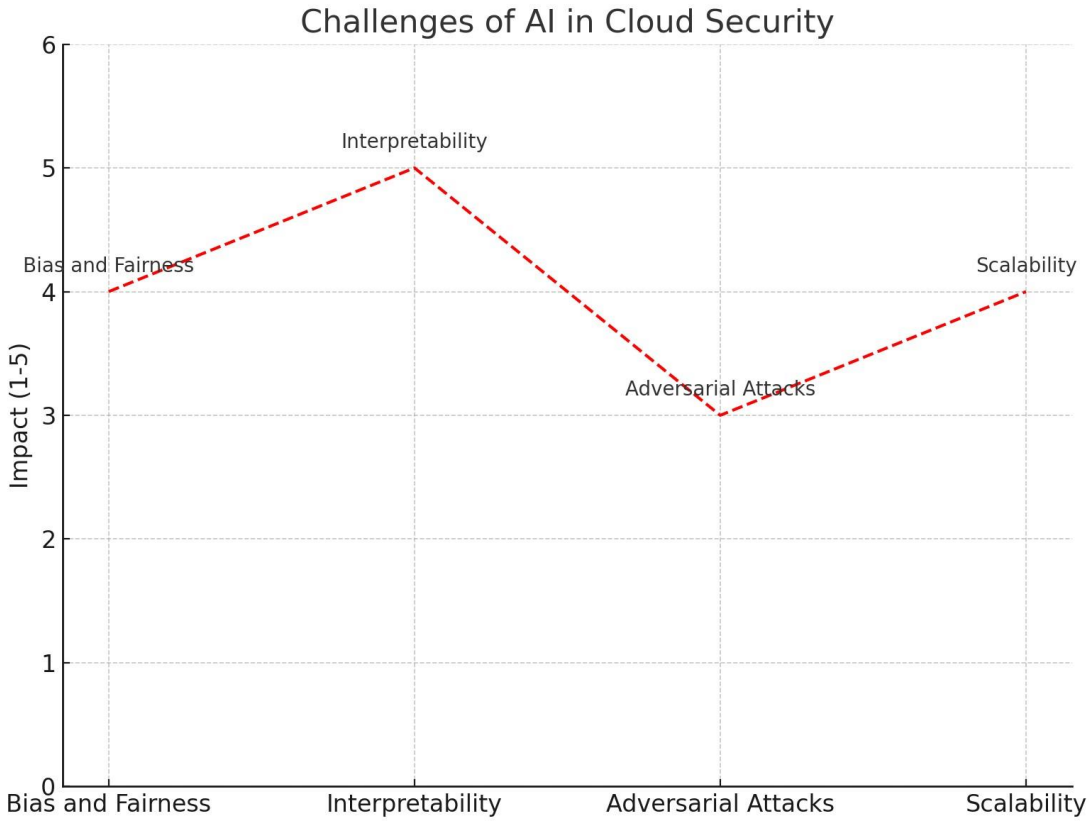

Figure 1. Challenges of AI in Cloud Security

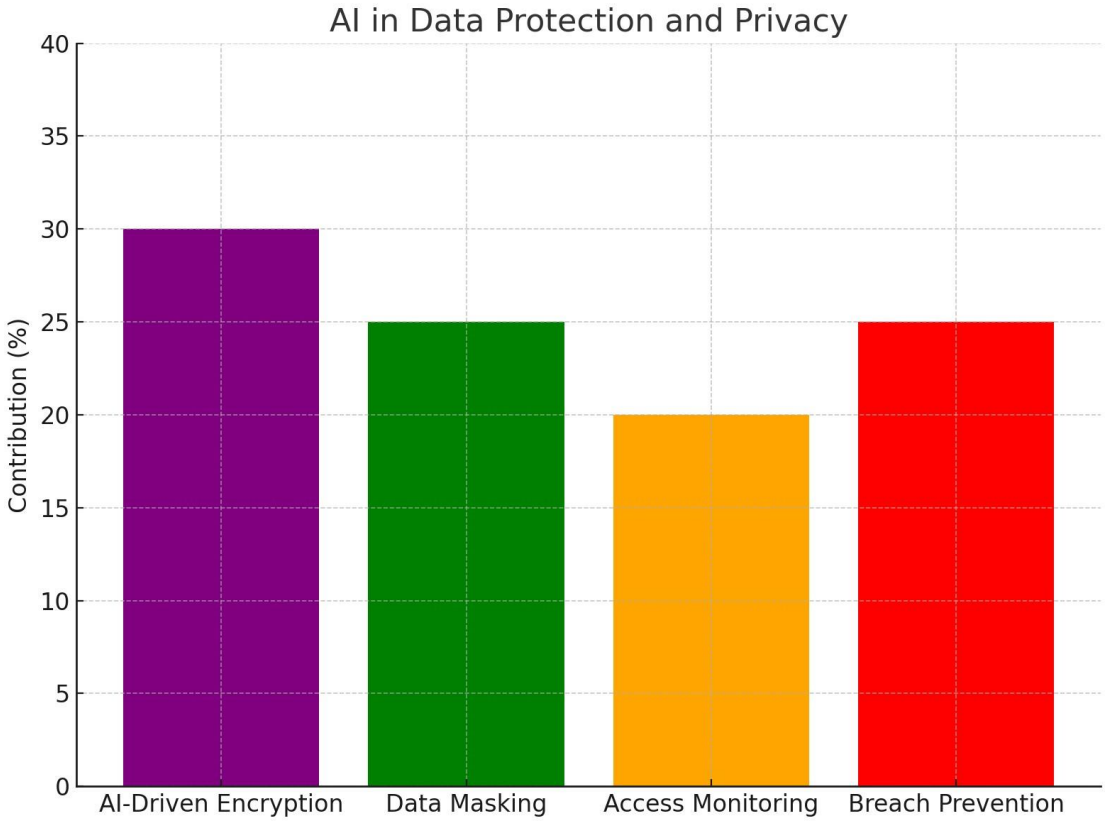

Figure 2. AI-in Data Protection and Privacy

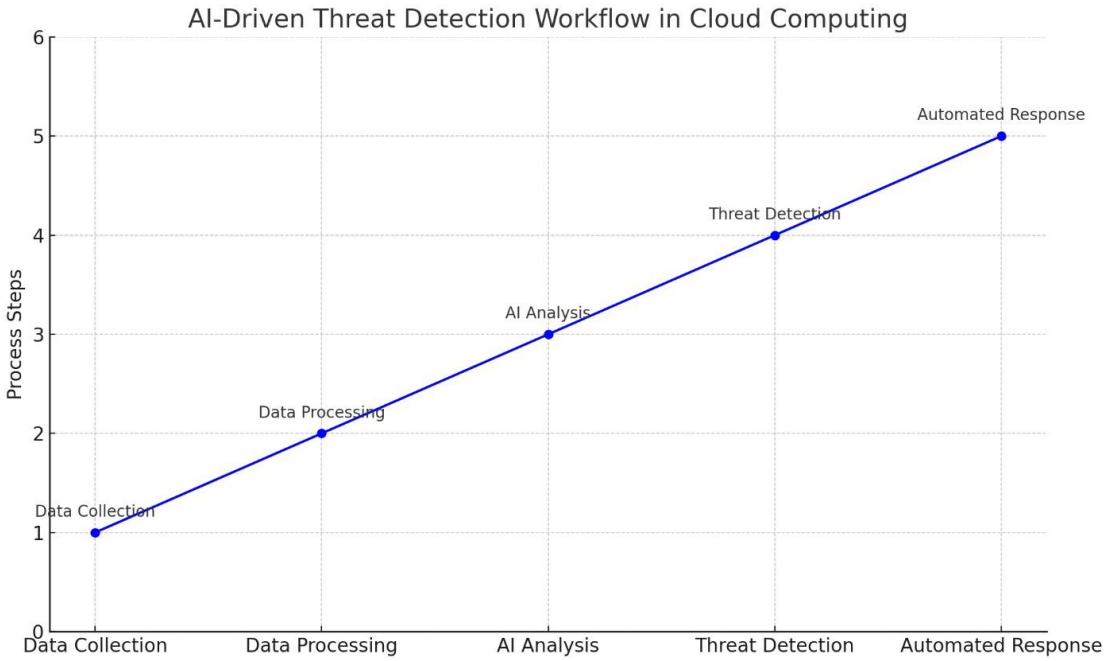

Figure 3. AI-Driven Threat Detection Workflow in Cloud Computing

2.4 Security Automation and Orchestration

AI enables the automation of security tasks, such as vulnerability scanning, patch management, and compliance monitoring. AI-powered Security Orchestration, Automation, and Response (SOAR) platforms can integrate various security tools and processes, providing a unified and automated approach to cloud security (Basharat & Omar, 2024).

C. Challenges of AI in Secure Cloud Computing

3.1 Bias and Fairness

AI models are only as good as the data they are trained on. If the training data is biased, the AI models will also exhibit bias, potentially leading to unfair or discriminatory security decisions (Burrell et al., 2022). This challenge is particularly significant in cloud environments where diverse user groups and data types are involved.

3.2 Interpretability and Transparency

AI models, especially those based on deep learning, are often criticized for their lack of transparency and interpretability. In cloud security, where understanding the rationale behind security decisions is crucial, this "black-box" nature of AI can be problematic (Omar & Burrell, 2024).

3.3 Adversarial Attacks

AI models are vulnerable to adversarial attacks, where malicious actors manipulate inputs to deceive the AI. In the context of cloud security, such attacks could lead to false positives or negatives, undermining the effectiveness of AI-driven security measures (Omar & Mohaisen, 2022).

3.4 Scalability and Complexity

Integrating AI into cloud security requires significant computational resources, which can be challenging to scale across large, distributed cloud environments. The complexity of managing AI-driven security tools can also lead to integration issues and increased operational overhead (Jones & Omar, 2024).

D. Case Studies

4.1 AI-Powered Threat Detection in Cloud Environments

This section could present a case study of an organization that successfully implemented AIdriven threat detection in its cloud infrastructure, highlighting the benefits and challenges encountered.

4.2 AI in Compliance Monitoring and Data Protection

This case study could explore how a financial institution uses AI to automate compliance monitoring and enhance data protection in its cloud environment.

E. Future Directions

5.1 Explainable AI for Cloud Security

Future research should focus on developing explainable AI models that provide transparency in decision-making processes, making it easier for security professionals to trust and validate AIdriven security measures (Omar & Sukthankar, 2023).

5.2 AI-Driven Security for Multi-Cloud Environments

As organizations increasingly adopt multi-cloud strategies, future research should explore AIdriven security solutions that can operate seamlessly across

multiple cloud providers, ensuring consistent security policies and threat detection capabilities.

5.3 Addressing AI Bias in Cloud Security

Research should continue to develop techniques for identifying and mitigating bias in AI models used in cloud security, ensuring that these models operate fairly and equitably (Gholami, 2024).

F. Conclusion

The integration of AI into cloud computing presents significant opportunities for enhancing security. However, these opportunities are accompanied by challenges that must be addressed to ensure the effectiveness and fairness of AI-driven security solutions. By focusing on areas such as explainable AI, multi-cloud security, and bias mitigation, the future of AI in secure cloud computing looks promising.

G. References

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

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

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

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

[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. CMESComputer 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,

[39] 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.
[40] 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.
[41] 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.
[42] 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.
[43] Jones, A., & Omar, M. (2024). Codesentry: Revolutionizing Real-Time Software Vulnerability Detection With Optimized GPT Framework. Land Forces Academy Review, 29(1), 98-107.
[44] 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.
[45] 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.
[46] 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.
[47] 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.
[48] 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.
[49] 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.
[50] Jones, R., Omar, M., & Mohammed, D. (2023). Harnessing the Power of the GPT Model to Generate Adversarial Examples. In 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) (pp. 16991702). IEEE.
[51] 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.
[52] 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.

[53] 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.
[54] 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.
[55] 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.
[56] Majeed, H. (2020). Watermarking Image Depending on Mojette Transform for Hiding
[57] Information. International Journal Of Computer Sciences And Engineering, 8, 8-12.
[58] Mohammed, D., & Omar, M. (2024). Decision Trees Unleashed: Simplifying IoT Malware Detection With Advanced AI Techniques. In Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology (pp. 240258). IGI Global.
[59] 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.
[60] 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.
[61] 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.
[62] 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.
[63] 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.
[64] Omar, M. & Zangana, H. M. (Eds.). (2024). Redefining Security With Cyber AI. IGI Global. https://doi.org/10.4018/979-8-3693-6517-5
[65] Omar, M. (2012). Smartphone Security: Defending Android-based Smartphone Against Emerging Malware Attacks (Doctoral dissertation, Colorado Technical University).
[66] 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.
[67] 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.
[68] Omar, M. (2019). A world of cyber attacks (a survey).

[69] Omar, M. (2021). Developing Cybersecurity Education Capabilities at Iraqi Universities.
[70] 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.
[71] 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.
[72] Omar, M. (2022). Machine Learning for Cybersecurity: Innovative Deep Learning Solutions. Springer Brief.
[73] https://link.springer.com/book/978303115
[74] 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.
[75] 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.
[76] 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.
[77] 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.
[78] Omar, M. (n.d.). Defending Cyber Systems through Reverse Engineering of Criminal Malware. Springer Brief.
[79] https://link.springer.com/book/9783031116278
[80] Omar, M. (n.d.). Latina Davis Morgan State University 1700 E Cold Spring Ln. Baltimore, MD 21251, USA E-mail: latinaedavis@ hotmail. com.
[81] Omar, M. (n.d.). Machine Learning for Cybersecurity.
[82] 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.
[83] 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.
[84] 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.
[85] 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).
[86] Omar, M., & Shiaeles, S. (2023). VulDetect: A novel technique for detecting software vulnerabilities using Language Models. In 2023 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE. https://ieeexplore.ieee.org/document/10224924

[87] 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.
[88] 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.
[89] 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).
[90] 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.
[91] 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.
[92] 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.
[93] 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).
[94] 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.
[95] 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.
[96] 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.
[97] 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.
[98] Saleem, M. A., Li, X., Mahmood, K., Shamshad, S., Ayub, M. F., & Omar, M. (2023). Provably secure conditionalprivacy access control protocol for intelligent customers-centric communication in vanet. IEEE Transactions on Consumer Electronics. IEEE.
[99] 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.
[100] 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.

[101] 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.
[102] 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.
[103] 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.
[104] 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.
[105] 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.
[106] 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.
[107] Zangana, H. M. (2017). A new algorithm for shape detection. IOSR Journal of Computer Engineering (IOSR-JCE), 19(3), 71-76.
[108] Zangana, H. M. (2017). Library Data Quality Maturity (IIUM as a Case Study). IOSR-JCE March, 29, 2017.
[109] Zangana, H. M. (2017). Watermarking System Using LSB. IOSR Journal of Computer Engineering, 19(3), 75-79.
[110] Zangana, H. M. (2018). Design an information management system for a pharmacy. International Journal of Advanced Research in Computer and Communication Engineering, 7(10).
[111] 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.
[112] 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.
[113] Zangana, H. M. (2018). Implementing a System for Recognizing Optical Characters.
[114] Zangana, H. M. (2019). Issues of Data Management in the Library: A Case Study.
[115] Zangana, H. M. (2019). ITD Data Quality Maturity (A Case Study). International Journal Of Engineering And Computer Science, 8(10).
[116] Zangana, H. M. (2020). Mobile Device Integration in IIUM Service. International Journal, 8(5).
[117] Zangana, H. M. (2021). The Global Finical Crisis from an Islamic Point Of View. Qubahan Academic Journal, 1(2), 55-59.
[118] Zangana, H. M. (2022). Creating a Community-Based Disaster Management System. Academic Journal of Nawroz University, 11(4), 234-244.
[119] Zangana, H. M. (2022). Implementing New Interactive Video Learning System for IIUM. Academic Journal of Nawroz University, 11(2), 23-29.

[120] 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).
[121] Zangana, H. M. (2024). Exploring Blockchain-Based Timestamping Tools: A Comprehensive Review. Redefining Security With Cyber AI, 92-110.
[122] Zangana, H. M. (2024). Exploring the Landscape of Website Vulnerability Scanners: A Comprehensive Review and Comparative Analysis. Redefining Security With Cyber AI, 111-129.
[123] Zangana, H. M. CHALLENGES AND ISSUES of MANET.
[124] 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.
[125] 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.
[126] Zangana, H. M., & Mustafa, F. M. (2024). From Classical to Deep Learning: A Systematic Review of Image Denoising Techniques. Jurnal Ilmiah Computer Science, 3(1), 50-65.
[127] 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).
[128] 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.
[129] Zangana, H. M., & Omar, M. (2020). Threats, Attacks, and Mitigations of Smartphone Security. Academic Journal of Nawroz University, 9(4), 324-332.
[130] Zangana, H. M., & Omar, M. (2020). Threats, Attacks, and Mitigations of Smartphone Security. Academic Journal of Nawroz University, 9(4), 324-332.
[131] 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.
[132] 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.
[133] 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.
[134] 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.
[135] 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.
[136] 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.

[137] 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.
[138] 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.
[139] 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).
[140] 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
[141] International Journal of Applied Business), 8(1), 88–103. https://doi.org/10.20473/tijab.v8.I1.2024.54618
[142] 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.
[143] Zangana, H. M., Omar, M., Al-Karaki, J. N., & Mohammed, D. (2024). Comprehensive Review and Analysis of Network Firewall Rule Analyzers: Enhancing Security Posture and Efficiency. In Redefining Security With Cyber AI (pp. 15-36). IGI Global.
[144] 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.
[145] 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.
[146] Zangana, H. M., Tawfiq, N. E., & Omar, M. (2020). Advantages and Challenges of E-Government in Turkey.
[147] Zangana[1], H. M., Tawfiq, N. E., & Omar, M. (2020). Advantages and Challenges of E-Government in Turkey.
[148] 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.
[149] Zhou, S., Ali, A., Al-Fuqaha, A., Omar, M., & Feng, L. (n.d.). Robust Risk-Sensitive Task Offloading for
[150] Edge-Enabled Industrial Internet of Things. IEEE Transactions on Consumer Electronics