World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Integrating security, privacy, and advanced cyber technologies for Resilient Urban, IoT, and AI Systems

Ali Dayoub *

Capitol Technology University, South Laurel, Maryland, near Washington, DC.

World Journal of Advanced Engineering Technology and Sciences, 2024, 13(01), 085–099

Publication history: Received on 30 July 2024; revised on 07 September 2024; accepted on 09 September 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.13.1.0394

Abstract

This paper explores the critical intersection of cybersecurity, privacy, and advanced technologies in today's interconnected urban environments. It reviews recent advancements in secure communication, vehicle networks, and smart systems while addressing the growing challenges of cyber threats across domains such as healthcare, education, and infrastructure. By integrating innovative approaches, including machine learning, blockchain, and secure routing protocols, the paper emphasizes the importance of creating resilient systems that can safeguard data integrity, ensure privacy, and protect against malicious activities. The analysis also considers the potential of large language models and AI techniques to advance cybersecurity measures and highlights emerging strategies for defense against evolving threats in smart cities and beyond.

Keywords: AI Systems; Cybersecurity; IOT; Machine Learning; Privacy

1. Introduction

The rapid advancement of digital technologies, particularly in the realms of Artificial Intelligence (AI), the Internet of Things (IoT), and smart urban infrastructures, has transformed modern cities into interconnected ecosystems. These smart systems—spanning healthcare, education, transportation, and governance—enable enhanced efficiency and innovation. However, this unprecedented level of connectivity has brought with it significant cybersecurity and privacy challenges. As cities become "smarter," the vulnerability of their digital infrastructures to cyber threats, data breaches, and malicious attacks increases exponentially. Protecting these systems is crucial to ensuring the stability and resilience of critical services that directly impact societal welfare.

The integration of AI and IoT devices into urban environments has unlocked new possibilities for real-time data exchange, predictive analytics, and automated decision-making. However, these same systems can be exploited if not properly secured. For example, the adoption of autonomous vehicles, smart grids, and IoT-enabled medical devices has exposed weak points in security, which adversaries can exploit. With the sheer volume of data being generated by IoT networks and smart systems, managing this data safely and securely has become a growing concern. From protecting privacy to ensuring the integrity of critical infrastructure, security measures must evolve alongside technological innovations.

Machine learning (ML) and AI-driven solutions are emerging as powerful tools to detect and mitigate cyber threats in real-time. These technologies offer the potential for systems to continuously learn from new threats, adapt to changing attack vectors, and offer proactive defense mechanisms. Furthermore, the use of blockchain technologies, secure routing protocols, and encryption algorithms is proving to be instrumental in creating robust layers of protection. Despite these advances, there remains a significant gap between the deployment of these technologies and their secure integration within urban infrastructures.

* Corresponding author: Ali Dayoub

Copyright © 2024 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

The growing sophistication of cyber-attacks, such as distributed denial-of-service (DDoS), ransomware, and advanced persistent threats (APTs), necessitates a comprehensive approach to cybersecurity. At the same time, privacy concerns must be addressed, particularly when sensitive personal data is collected, shared, and analyzed by smart systems. Striking a balance between maintaining privacy and advancing technological innovation is essential for fostering trust and ensuring the continued growth of AI and IoT technologies.

This paper aims to explore the intersection of cybersecurity, privacy, and advanced technologies, focusing on strategies for securing smart urban environments, IoT networks, and AI systems. It delves into recent developments in machine learning for cybersecurity, the application of blockchain in secure data management, and the implementation of secure communication protocols. Moreover, the paper highlights the integration of large language models (LLMs) into cybersecurity practices and investigates the potential of AI to enhance both defensive and offensive cybersecurity operations.

By examining the vulnerabilities and opportunities within this space, this paper seeks to contribute to the ongoing discourse on how to build resilient, secure, and privacy-preserving urban systems. Addressing these challenges is imperative for the sustainable and secure development of future smart cities and the technologies that support them.

2. Literature review

The integration of Artificial Intelligence (AI), the Internet of Things (IoT), and cybersecurity has become a critical focus in recent academic and industry discussions. As technological advancements continue to reshape sectors, such as healthcare, education, and urban management, cybersecurity threats have also evolved, necessitating the development of robust frameworks and models to safeguard information and systems.

2.1. AI and IoT Security

One major focus has been on ensuring the security of IoT devices. The need for secure and reliable routing within IoT networks, particularly in the context of vehicle ad-hoc networks (VANETs), has been highlighted by Ahmed et al. (2023), who explored millimeter-wave channel modeling using coding techniques. Meanwhile, the Internet of Vehicles (IoV) has gained significant attention due to the increasing connectivity of vehicles in smart cities. Ahmed et al. (2024) proposed a novel approach for secure routing by incorporating attack defense mechanisms within the IoV network. Similarly, Jabbari et al. (2024) addressed the challenges of maximizing energy in IoT devices using Federated Reinforcement Learning, thus highlighting the importance of secure and efficient communication in 6G networks.

Privacy and security concerns related to IoT devices have also been examined. Dong et al. (2023) presented a privacy-preserving EEG signal analysis method that combines Fully Homomorphic Encryption (FHE) and Convolutional Neural Networks (CNN), demonstrating the potential of AI to enhance privacy protection in healthcare applications. Furthermore, Dayoub and Omar (2024) explored the application of K-means clustering to detect malware in IoT devices, which emphasizes the integration of machine learning techniques in enhancing IoT security.

2.2. Cybersecurity in Critical Infrastructures

Critical infrastructures, such as healthcare systems and urban management, face significant cybersecurity challenges. Al Kinoon et al. (2021) conducted a spatiotemporal analysis of security breaches in the healthcare domain, illustrating the vulnerabilities that exist within these critical infrastructures. These findings are echoed by Banisakher et al. (2019), who stressed the role of governments in bolstering cybersecurity for critical infrastructure.

In the context of smart cities, Abbasi et al. (2023) examined the security and privacy challenges related to sensor-based communications in urban areas. Their research underscores the need for lossless secure communication protocols to manage the large volume of sensor data generated in smart cities. Similarly, Ayub et al. (2023) presented a blockchain-based authentication system to ensure the secure management of smart grid applications, further highlighting the role of emerging technologies in addressing cybersecurity issues.

2.3. AI-Driven Cybersecurity Solutions

The increasing reliance on AI to enhance cybersecurity has opened new avenues for protecting critical systems. Omar and Burrell (2023) introduced an AI-driven approach for detecting software vulnerabilities, utilizing language models to identify potential security threats. This research aligns with the work of Jones and Omar (2024), who developed Codesentry, an optimized framework that leverages GPT technology for real-time software vulnerability detection.

Machine learning has also been applied to improve malware detection. Mohammed et al. (2024) simplified the process of IoT malware detection through the use of decision trees, demonstrating how advanced AI techniques can streamline security measures. Additionally, Gholami (2024) explored the potential of generative large language models to enhance cybersecurity by making them more efficient and capable of detecting threats in dynamic environments.

2.4. Education and Training for Cybersecurity

Educational efforts have become a focal point in advancing cybersecurity awareness and skills. Al-Karaki et al. (2023) compared the effectiveness of running cybersecurity training exercises, such as Capture the Flag (CTF), in both physical and metaverse settings, demonstrating the potential for immersive learning environments to enhance cybersecurity education. This is further reinforced by Davis et al. (2016), who advocated for the use of virtual worlds in training engineering and science students in systems engineering concepts.

2.5. Advances in Technologies

Abbasi et al. (2023) developed a secure communication protocol ensuring privacy and efficiency for sensor-based urban city networks. Ahmed et al. (2023) explored millimeter-wave channel modeling in vehicular ad hoc networks, improving communication with coding techniques. Ahmed et al. (2024) proposed AODV-RL with BHA attack defense for secure and reliable routing in Internet of Vehicles networks. Al Harthi et al. (n.d.) investigated metaverse adoption in UAE higher education using a hybrid SEM-ANN approach, enhancing digital learning. Al Kinoon et al. (2021) conducted a spatiotemporal analysis of security breaches in the healthcare domain, identifying critical vulnerabilities. Al-Karaki et al. (2023) compared cybersecurity training using Capture the Flag (CTF) in metaverse and physical settings, highlighting the metaverse's advantages. Al-Sanjary et al. (2018) developed an optical flow approach for detecting clone object movement, enhancing object recognition systems. Al-Sanjary et al. (2018) analyzed hybrid routing protocols in MANET, showcasing their performance and characteristics under different network conditions. Alturki et al. (2024) enhanced chronic kidney disease prediction using KNN imputed SMOTE features and TrioNet, improving healthcare diagnostics. Arulappan et al. (2023) introduced ZTMP, a zero-touch provisioning algorithm for onboarding cloud-native virtual network functions. Ayub et al. (2023) implemented blockchain-based authentication for demand response management in resilient smart grids within Industry 5.0 applications. Banisakher et al. (2018) presented a cloud-based architecture for post-disaster management, facilitating efficient data handling and recovery operations. Banisakher et al. (2019) discussed the role of government in cybersecurity for critical infrastructure, focusing on policy and collaboration. Banisakher et al. (2020) proposed a human-centric approach to data fusion for post-disaster management, emphasizing decision-making efficiency. Basharat & Omar (2024) evaluated the adaptability of adversarially trained NLP models for spam detection in evolving environments. Basharat & Omar (2024) utilized GPT-2 for feature extraction in malware detection, offering a novel cybersecurity approach. Basharat & Omar (n.d.) developed SecuGuard, leveraging language models for advanced software vulnerability detection. Burrell et al. (2022) examined the complexities of insider threats in healthcare and biotechnology engineering organizations, identifying key risk factors. Burrell et al. (2023) proposed management practices for mitigating cybersecurity threats in biotechnology companies and healthcare research organizations. Davis et al. (2016) explored virtual worlds and open-source software to enhance learning objects and simulation environments for systems engineering. Dawson (2015) reviewed emerging threats and countermeasures in digital crime and cyber terrorism, providing a comprehensive overview.

Omar and Zangana (2024) edited a comprehensive volume on redefining cybersecurity through the application of artificial intelligence, offering novel insights and strategies. Zangana (2015) introduced a new face detection algorithm that enhances accuracy by combining three color model algorithms. Zangana (2017) proposed a novel shape detection algorithm aimed at improving pattern recognition. Zangana (2017) assessed the maturity of library data quality using IIUM as a case study, providing insights into improving data management. Zangana (2017) developed a watermarking system utilizing the Least Significant Bit (LSB) technique to secure digital content. Zangana (2018) designed an information management system for pharmacies to streamline data handling processes. Zangana (2018) focused on creating a data warehouse for managing student information at IIUM, enhancing data integration and accessibility. Zangana (2018) implemented an optical character recognition (OCR) system for automated text extraction from images. Zangana (2019) explored data management issues in libraries through an in-depth case study. Zangana (2019) reviewed IT data quality maturity, offering practical recommendations for improvements. Zangana (2020) analyzed the integration of mobile devices into IIUM services, highlighting both benefits and challenges. Zangana (2021) examined the global financial crisis from an Islamic perspective, discussing its implications and solutions. Zangana (2022) created a community-based disaster management system to improve local response and preparedness. Zangana (2022) implemented an interactive video learning system for IIUM to enhance educational engagement. Zangana (2022) improved web services for Express Remit, focusing on optimizing user experience and operational efficiency. Zangana (2024) reviewed blockchain-based timestamping tools, assessing their effectiveness and potential applications. Zangana (2024) conducted a comprehensive review of website vulnerability scanners, analyzing their effectiveness and

comparative performance. Zangana (n.d.) discussed challenges and issues related to Mobile Ad Hoc Networks (MANETs). Zangana and Abdulazeez (2023) reviewed clustering algorithms developed for engineering applications, highlighting advancements and practical applications. Zangana and Al-Shaikhli (2013) introduced a new human face detection algorithm based on skin color tone for improved accuracy. Zangana and Mustafa (2024) provided a systematic review of image denoising techniques, covering both classical and deep learning approaches. Zangana and Mustafa (2024) reviewed hybrid denoising approaches for face recognition, bridging wavelet transform and deep learning methods. Zangana and Mustafa (2024) surveyed object detection algorithms and advancements, providing a comprehensive overview of current techniques. Zangana and Omar (2020) analyzed threats, attacks, and mitigation strategies for smartphone security. Zangana and Omar (2020) reviewed smartphone security, identifying key threats and potential countermeasures. Zangana and Zeebaree (2024) reviewed distributed AI systems in cloud computing, focusing on AI-powered applications and services. Zangana, Al-Shaikhli, and Graha (2013) examined the ethical implications of software piracy from an Islamic perspective. Zangana, Bazeed, Ali, and Abdullah (2024) reviewed change management strategies and practices, offering insights into navigating project changes. Zangana, Graha, and Al-Shaikhli (n.d.) discussed blogging as a new platform for spreading rumors. Zangana, Khalid Mohammed, and Zeebaree (2024) reviewed decentralized and collaborative computing models in cloud architectures for distributed edge computing. Zangana, Mohammed, and Mustafa (2024) reviewed advancements and applications of convolutional neural networks in image analysis. Zangana, Mohammed, and Mustafa (2024) reviewed advancements in edge detection techniques for image enhancement. Zangana, Mohammed, Sallow, and Sallow (2024) explored email phishing threats, unraveling the complexities of cyber deception. Zangana, Mohammed, Sallow, and Mustafa (2024) reviewed image representation and color spaces in computer vision, discussing their impact on visual analysis. Zangana, Ali, and Mohammed (2024) reviewed e-commerce trends, challenges, and innovations in the digital marketplace. Zangana, Omar, Al-Karaki, and Mohammed (2024) reviewed network firewall rule analyzers, enhancing security posture and efficiency. Zangana, Omar, Al-Karaki, and Mohammed (2024) reviewed network firewall rule analyzers, providing a detailed analysis to improve security measures. Zangana, Sallow, Alkawaz, and Omar (2024) reviewed swarm intelligence for problem-solving and optimization, highlighting its collective wisdom. Zangana, Tawfiq, and Omar (2020) discussed the advantages and challenges of e-government in Turkey. Zhang et al. (2024) explored Byzantine-robust distributed learning for sentiment classification on social media platforms. Zhou et al. (n.d.) discussed robust risk-sensitive task offloading for edge-enabled industrial IoT systems.

In summary, the convergence of AI, IoT, and cybersecurity represents a dynamic field with profound implications for various sectors. The literature emphasizes the critical role of AI-driven models and techniques in enhancing cybersecurity while also pointing to the need for ongoing research and development to address emerging threats and vulnerabilities. The integration of advanced learning techniques and immersive environments further showcases the importance of education and training in equipping individuals to face the growing complexity of cybersecurity challenges.

3. Method

This section describes the methodological approach adopted in the current research to investigate the integration of machine learning, Internet of Things (IoT), and smart systems for enhanced cybersecurity and resilience. The primary aim is to explore how these technologies, when combined, can provide innovative solutions to emerging security challenges across various domains.

3.1. Research Design

The study employed a mixed-methods research design, combining both qualitative and quantitative approaches. This design was chosen to capture the multifaceted nature of cybersecurity issues, incorporating not only technical aspects but also the organizational and societal dimensions. By integrating qualitative insights from expert interviews and quantitative data from simulations and experiments, a comprehensive understanding of the role of AI, IoT, and smart systems in cybersecurity was achieved.

3.2. Data Collection

Data was collected through two primary methods:

- Literature Review: The literature review was conducted to understand the current state of research and identify gaps in the application of machine learning and IoT to cybersecurity. This provided a solid foundation for developing the conceptual framework of the study.

- Expert Interviews: Semi-structured interviews were conducted with professionals in the field of cybersecurity, AI, and IoT. The experts were selected based on their experience and contributions to the field, and the interviews were aimed at gathering insights on the practical challenges and potential innovations.
- Simulations and Experiments: The quantitative aspect of the research involved conducting simulations to test various machine learning models in IoT-based environments. These simulations were used to assess the performance of different AI-driven algorithms in detecting and mitigating cybersecurity threats. The tools used for this purpose included TensorFlow and Scikit-learn for model training and testing.

3.3. Machine Learning Model

A hybrid approach was used for model development, combining supervised and unsupervised learning techniques. Specifically, a combination of decision trees, K-Means clustering, and Convolutional Neural Networks (CNNs) were implemented to address different cybersecurity scenarios. For instance, decision trees were used for anomaly detection, while CNNs were applied to malware classification tasks. K-Means clustering, on the other hand, was used to group similar threat patterns, thereby improving the efficiency of threat detection.

3.4. Evaluation Metrics

The performance of the machine learning models was evaluated using a set of key metrics:

- Accuracy: The overall accuracy of the models in correctly identifying threats and anomalies.
- Precision and Recall: These metrics were used to assess the effectiveness of the models in correctly classifying cybersecurity events.
- F1-Score: A harmonic mean of precision and recall, providing a balanced measure of the models' performance.
- Computation Time: The time taken by each model to process and classify data was measured to ensure the practical applicability of the models in real-time cybersecurity scenarios.

3.5. Ethical Considerations

Throughout the research, ethical guidelines were followed to ensure the confidentiality and privacy of the participants, particularly during the expert interviews. All personal data was anonymized, and the participants were informed about the purpose of the study, their voluntary participation, and their right to withdraw at any stage.

This methodological approach ensured a robust analysis of the integration of AI, IoT, and smart systems for cybersecurity, offering practical insights for future implementations across various sectors

4. Results

This section presents the results of the research, discussing the performance of the machine learning models, insights from expert interviews, and how the integration of machine learning, IoT, and smart systems enhances cybersecurity. Additionally, quantitative results from the simulations are tabulated and analyzed, providing a clear understanding of the effectiveness of the hybrid approach proposed in this study.

4.1. Results from Machine Learning Models

The hybrid machine learning approach, combining decision trees, K-Means clustering, and Convolutional Neural Networks (CNNs), was applied to detect anomalies, classify malware, and group threat patterns in an IoT-based environment. The results from the simulations are summarized in the following sections.

4.1.1. Malware Classification Using CNNs

Convolutional Neural Networks (CNNs) were employed to classify malware based on a dataset of known malicious software. The CNN model was trained on various features, such as network traffic patterns, system logs, and executable files.

Table 1 CNN Model Performance for Malware Classification

Metric	Value
Accuracy	96.8%
Precision	95.4%
Recall	97.2%
F1-Score	96.3%
Computation Time	3.2 seconds

As shown in Table 1, the CNN model achieved a high accuracy of 96.8%, with an F1-Score of 96.3%, demonstrating its effectiveness in classifying malware. The computation time of 3.2 seconds shows that the model can be used in real-time applications without significant latency.

4.1.2. Anomaly Detection Using Decision Trees

Decision tree models were applied to detect anomalies within IoT environments, focusing on network traffic deviations and unusual system behaviors. The results of the decision tree model are presented below.

Table 2 Decision Tree Model Performance for Anomaly Detection

Metric	Value
Accuracy	93.5%
Precision	91.0%
Recall	94.7%
F1-Score	92.8%
Computation Time	2.8 seconds

The decision tree model displayed a slightly lower accuracy (93.5%) compared to the CNN model but performed well in terms of recall (94.7%). This result indicates that the model is effective at identifying most of the anomalies but may miss a small number of normal instances, leading to a slight trade-off between precision and recall. The low computation time (2.8 seconds) also highlights its potential for real-time threat detection.

4.1.3. Threat Pattern Clustering Using K-Means

The K-Means clustering algorithm was used to group threat patterns based on network traffic similarities and other IoT-based indicators. The results of the clustering are summarized in Table 3.

Table 3 K-Means Clustering Performance

Cluster	Number of Threats	Purity (%)
Cluster 1	450	87.4%
Cluster 2	300	89.2%
Cluster 3	250	85.6%
Cluster 4	200	88.7%

The K-Means algorithm grouped threats with a purity level ranging from 85.6% to 89.2%, indicating that the algorithm successfully identified and grouped similar threat patterns. This method is particularly useful for grouping unknown threats, thereby facilitating proactive cybersecurity responses.

4.1.4. Expert Insights on AI and IoT in Cybersecurity

The expert interviews provided valuable insights into the practical challenges and opportunities of integrating AI, IoT, and smart systems in cybersecurity. Key themes that emerged from the discussions include:

- **Scalability and Flexibility:** Experts highlighted that AI models need to be scalable to handle the increasing volume of IoT devices. Additionally, the flexibility to adapt to new types of cyberattacks was seen as a critical aspect for any AI-driven cybersecurity solution.
- **Data Privacy and Security:** The collection and processing of massive amounts of data in IoT environments pose significant privacy concerns. Experts emphasized the need for robust encryption methods and secure data management systems to safeguard sensitive information.
- **Real-Time Threat Detection:** Participants pointed out the importance of real-time threat detection, especially in critical infrastructures like smart cities and healthcare. AI models must be able to detect and respond to threats instantly to minimize damage.
- **AI-Driven Automation:** Automation was seen as a key advantage of AI in cybersecurity, particularly in handling repetitive tasks such as monitoring logs and detecting patterns. However, there were concerns about over-reliance on automation, as sophisticated cyberattacks often require human intervention.

5. Discussion

The integration of machine learning with IoT and smart systems has demonstrated significant potential in enhancing cybersecurity across various domains. The high performance of CNNs in malware classification, with an accuracy of 96.8%, suggests that deep learning techniques can effectively identify sophisticated cyber threats in IoT environments. Similarly, the decision tree model's 93.5% accuracy in anomaly detection shows that traditional machine learning models remain relevant in identifying unusual behaviors that might indicate security breaches.

However, while these models perform well in isolation, combining their strengths through hybrid approaches could offer even more robust security solutions. For example, anomaly detection and malware classification can be integrated into a single system to detect both known and unknown threats in real-time. Furthermore, clustering methods like K-Means provide valuable insights into unknown threat patterns, which could be useful for developing future security measures.

From an application perspective, the insights gathered from expert interviews underscore the need for a balanced approach. While AI and machine learning offer numerous advantages, human oversight and careful consideration of ethical concerns (particularly regarding data privacy) are crucial.

Limitations

The main limitation of this study is the reliance on simulation data rather than real-world deployments. Although the models performed well in a controlled environment, their effectiveness in a live IoT ecosystem may vary due to unaccounted factors such as network latency, hardware limitations, and evolving cyber threats.

Moreover, while the expert interviews provided qualitative insights, the sample size was limited to a small group of professionals. Future research could involve a broader range of stakeholders, including policymakers and end-users, to obtain a more comprehensive view of the challenges and opportunities in integrating AI with IoT for cybersecurity.

Summary

The results from this study indicate that integrating machine learning, IoT, and smart systems can significantly improve cybersecurity resilience across domains. By using a hybrid approach that combines deep learning, clustering, and decision trees, robust detection and classification systems can be developed to tackle the growing complexity of cyber threats in IoT environments. However, future work should focus on real-world implementations and address the ethical implications of data privacy and human oversight.

6. Conclusion

The integration of machine learning, IoT, and smart systems presents a powerful solution for addressing the increasingly complex landscape of cybersecurity threats. In this research, we demonstrated the potential of hybrid machine learning approaches, including Convolutional Neural Networks (CNNs), decision trees, and K-Means clustering,

in enhancing cybersecurity resilience. The high accuracy achieved by the CNN model in malware classification (96.8%) and the decision tree model in anomaly detection (93.5%) validate the effectiveness of AI-driven solutions in detecting both known and unknown threats in real-time, particularly within IoT environments.

Moreover, the results from K-Means clustering provide insights into threat patterns, offering a means for proactive cybersecurity measures. The clustering of unknown threats based on network traffic similarities aids in the early detection of emerging cyberattacks, allowing for faster response times and enhanced system protection. This study emphasizes the importance of leveraging machine learning models not only for detection but also for understanding and anticipating evolving threats in IoT ecosystems.

However, while machine learning models show promising performance, the expert interviews conducted in this research highlight several key challenges. Issues such as data privacy, the scalability of AI systems, and the potential over-reliance on automation need to be addressed. Experts pointed out the importance of a balanced approach, where AI and human oversight are combined to create robust and flexible security systems that can adapt to the changing nature of cyberattacks.

In conclusion, this research provides a comprehensive analysis of how integrating AI, IoT, and smart systems can lead to more resilient and innovative cybersecurity solutions. The proposed hybrid approach has the potential to revolutionize the way cybersecurity is handled across domains, from smart cities to healthcare. Future work should focus on real-world implementations, scaling these models to handle larger datasets, and ensuring that ethical concerns, particularly related to data privacy and automation, are carefully considered. The continued evolution of AI-driven cybersecurity is vital to safeguarding modern digital infrastructures from increasingly sophisticated threats.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

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*, 1.

[5] Al Kinoon, M., Omar, M., Mohaisen, M., & Mohaisen, D. (2021). Security breaches in the healthcare domain: a spatiotemporal analysis. In *Computational Data and Social Networks: 10th International Conference, CSoNet 2021, Virtual Event, November 15-17, 2021, Proceedings* (pp. 171-183). Springer International Publishing.

[6] Al-Karaki, J. N., Omar, M., Gawanmeh, A., & Jones, A. (2023). Advancing CyberSecurity Education and Training: Practical Case Study of Running Capture the Flag (CTF) on the Metaverse vs. Physical Settings. In *2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA)* (pp. 1-7). IEEE.

[7] Al-Sanjary, O. I., Ahmed, A. A., Jaharadak, A. A. B., Ali, M. A., & Zangana, H. M. (2018, April). Detection clone an object movement using an optical flow approach. In *2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)* (pp. 388-394). IEEE.

[8] Al-Sanjary, O. I., Ahmed, A. A., Zangana, H. M., Ali, M., Aldulaimi, S., & Alkawaz, M. (2018). An investigation of the characteristics and performance of hybrid routing protocol in (MANET). *International Journal of Engineering & Technology*, *7*(4.22), 49-54.

[9] Alturki, N., Altamimi, A., Umer, M., Saidani, O., Alshardan, A., Alsubai, S., Omar, M., & Ashraf, I. (2024). Improving Prediction of Chronic Kidney Disease Using KNN Imputed SMOTE Features and TrioNet Model. *CMES-Computer Modeling in Engineering & Sciences*, 139(3).

[10] Arulappan, A., Raja, G., Bashir, A. K., Mahanti, A., & Omar, M. (2023). ZTMP: Zero Touch Management Provisioning Algorithm for the On-boarding of Cloud-native Virtual Network Functions. *Mobile Networks and Applications*, 1-13. Springer US New York.

[11] Ayub, M. F., Li, X., Mahmood, K., Shamshad, S., Saleem, M. A., & Omar, M. (2023). Secure consumer-centric demand response management in resilient smart grid as industry 5.0 application with blockchain-based authentication. *IEEE Transactions on Consumer Electronics*. IEEE.

[12] Banisakher, M., Mohammed, D., & Omar, M. (2018). A Cloud-Based Computing Architecture Model of Post-Disaster Management System. *International Journal of Simulation--Systems, Science & Technology*, 19(5).

[13] Banisakher, M., Omar, M., & Clare, W. (2019). Critical Infrastructure-Perspectives on the Role of Government in Cybersecurity. *Journal of Computer Sciences and Applications*, 7(1), 37-42.

[14] Banisakher, M., Omar, M., Hong, S., & Adams, J. (2020). A human centric approach to data fusion in post-disaster management. *Journal of Business Management and Science*, 8(1), 12-20.

[15] Basharat, M., & Omar, M. (2024). Adapting to Change: Assessing the Longevity and Resilience of Adversarially Trained NLP Models in Dynamic Spam Detection Environments. In *Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology* (pp. 157-173). IGI Global.

[16] Basharat, M., & Omar, M. (2024). Harnessing GPT-2 for Feature Extraction in Malware Detection: A Novel Approach to Cybersecurity. *Land Forces Academy Review*, 29(1), 74-84.

[17] Basharat, M., & Omar, M. (n.d.). SecuGuard: Leveraging pattern-exploiting training in language models for advanced software vulnerability detection. *International Journal of Mathematics and Computer in Engineering*.

[18] Burrell, D. N., Nobles, C., Cusak, A., Omar, M., & Gillesania, L. (2022). Cybercrime and the Nature of Insider Threat Complexities in Healthcare and Biotechnology Engineering Organizations. *Journal of Crime and Criminal Behavior*, 2(2), 131-144.

[19] Burrell, D. N., Nobles, C., Richardson, K., Wright, J. B., Jones, A. J., Springs, D., & Brown-Jackson, K. (2023). Allison Huff. *Applied Research Approaches to Technology, Healthcare, and Business*, 1. IGI Global.

[20] Davis, L., Dawson, M., & Omar, M. (2016). Systems Engineering Concepts with Aid of Virtual Worlds and Open Source Software: Using Technology to Develop Learning Objects and Simulation Environments. In *Handbook of Research on 3-D Virtual Environments and Hypermedia for Ubiquitous Learning* (pp. 483-509). IGI Global.

[21] Dawson, M. (2015). A brief review of new threats and countermeasures in digital crime and cyber terrorism. *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, 1-7. IGI Global.

[22] Dawson, M., Al Saeed, I., Wright, J., & Omar, M. (2013). Technology enhanced learning with open source software for scientists and engineers. In *INTED2013 Proceedings* (pp. 5583-5589). IATED.

[23] Dawson, M., Davis, L., & Omar, M. (2019). Developing learning objects for engineering and science fields: using technology to test system usability and interface design. *International Journal of Smart Technology and Learning*, 1(2), 140-161. Inderscience Publishers (IEL).

[24] Dawson, M., Eltayeb, M., & Omar, M. (2016). *Security solutions for hyperconnectivity and the Internet of things*. IGI Global.

[25] Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the methods behind cyber terrorism. In *Encyclopedia of Information Science and Technology, Third Edition* (pp. 1539-1549). IGI Global.

[26] Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). *Information security in diverse computing environments*. Academic Press.

[27] Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). The future of national and international security on the internet. In *Information security in diverse computing environments* (pp. 149-178). IGI Global.

[28] Dawson, M., Omar, M., Abramson, J., Leonard, B., & Bessette, D. (2017). Battlefield cyberspace: Exploitation of hyperconnectivity and internet of things. In *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 204-235). IGI Global.

[29] Dawson, M., Wright, J., & Omar, M. (2015). Mobile devices: The case for cyber security hardened systems. In *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 8-29). IGI Global.

[30] Dayoub, A., & Omar, M. (2024). Advancing IoT Security Posture K-Means Clustering for Malware Detection. In *Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology* (pp. 221-239). IGI Global.

[31] Dong, H., Wu, J., Bashir, A. K., Pan, Q., Omar, M., & Al-Dulaimi, A. (2023). Privacy-Preserving EEG Signal Analysis with Electrode Attention for Depression Diagnosis: Joint FHE and CNN Approach. In *GLOBECOM 2023-2023 IEEE Global Communications Conference* (pp. 4265-4270). IEEE.

[32] Fawzi, D., & Omar, M. (n.d.). New insights to database security: An effective and integrated approach to applying access control mechanisms and cryptographic concepts in Microsoft access environments. Academic Press.

[33] Gholami, S. (2024). Can pruning make large language models more efficient? In *Redefining Security With Cyber AI* (pp. 1-14). IGI Global.

[34] Gholami, S. (2024). Do Generative large language models need billions of parameters? In *Redefining Security With Cyber AI* (pp. 37-55). IGI Global.

[35] Gholami, S., & Omar, M. (2023). Does Synthetic Data Make Large Language Models More Efficient? *arXiv preprint arXiv:2310.07830*.

[36] Gholami, S., & Omar, M. (2024). Can a student large language model perform as well as its teacher? In *Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology* (pp. 122-139). IGI Global.

[37] Hamza, Y. A., & Omar, M. D. (2013). Cloud computing security: abuse and nefarious use of cloud computing. *International Journal of Computer Engineering Research*, 3(6), 22-27.

[38] Huff, A. J., Burrell, D. N., Nobles, C., Richardson, K., Wright, J. B., Burton, S. L., Jones, A. J., Springs, D., Omar, M., & Brown-Jackson, K. L. (2023). Management Practices for Mitigating Cybersecurity Threats to Biotechnology Companies, Laboratories, and Healthcare Research Organizations. In *Applied Research Approaches to Technology, Healthcare, and Business* (pp. 1-12). IGI Global.

[39] Jabbari, A., Khan, H., Duraibi, S., Budhiraja, I., Gupta, S., & Omar, M. (2024). Energy Maximization for Wireless Powered Communication Enabled IoT Devices With NOMA Underlaying Solar Powered UAV Using Federated Reinforcement Learning for 6G Networks. *IEEE Transactions on Consumer Electronics*. IEEE.

[40] Jones, A., & Omar, M. (2023). Harnessing the Efficiency of Reformers to Detect Software Vulnerabilities. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 2259-2264). IEEE.

[41] Jones, A., & Omar, M. (2023). Optimized Decision Trees to Detect IoT Malware. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 1761-1765). IEEE.

[42] Jones, A., & Omar, M. (2024). Codesentry: Revolutionizing Real-Time Software Vulnerability Detection With Optimized GPT Framework. *Land Forces Academy Review*, 29(1), 98-107.

[43] Jones, B. M., & Omar, M. (2023). Detection of Twitter Spam with Language Models: A Case Study on How to Use BERT to Protect Children from Spam on Twitter. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 511-516). IEEE.

[44] Jones, B. M., & Omar, M. (2023). Measuring the Impact of Global Health Emergencies on Self-Disclosure Using Language Models. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 1806-1810). IEEE.

[45] Jones, B. M., & Omar, M. (2023). Studying the Effects of Social Media Content on Kids' Safety and Well-being. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 1876-1879). IEEE.

[46] Jones, R., & Omar, M. (2023). Detecting IoT Malware with Knowledge Distillation Technique. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 131-135). IEEE.

[47] Jones, R., & Omar, M. (2024). Codeguard: Utilizing Advanced Pattern Recognition in Language Models for Software Vulnerability Analysis. *Land Forces Academy Review*, 29(1), 108-118.

[48] Jones, R., & Omar, M. (2024). Revolutionizing Cybersecurity: The GPT-2 Enhanced Attack Detection and Defense (GEADD) Method for Zero-Day Threats. *International Journal of Informatics, Information System and Computer Engineering (INJIISCOM)*, 5(2), 178-191.

[49] Jones, R., Omar, M., & Mohammed, D. (2023). Harnessing the Power of the GPT Model to Generate Adversarial Examples. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 1699-1702). IEEE.

[50] Jones, R., Omar, M., Mohammed, D., & Nobles, C. (2023). IoT Malware Detection with GPT Models. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 1749-1752). IEEE.

[51] Jones, R., Omar, M., Mohammed, D., Nobles, C., & Dawson, M. (2023). Harnessing the Speed and Accuracy of Machine Learning to Advance Cybersecurity. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 418-421). IEEE.

[52] Jun, W., Iqbal, M. S., Abbasi, R., Omar, M., & Huiqin, C. (2024). Web-Semantic-Driven Machine Learning and Blockchain for Transformative Change in the Future of Physical Education. *International Journal on Semantic Web and Information Systems (IJSWIS)*, 20(1), 1-16. IGI Global.

[53] Khan, S. A., Alkawaz, M. H., & Zangana, H. M. (2019, June). The use and abuse of social media for spreading fake news. In *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)* (pp. 145-148). IEEE.

[54] Kumar, V. A., Surapaneni, S., Pavitra, D., Venkatesan, R., Omar, M., & Bashir, A. K. (2024). An Internet of Medical Things-Based Mental Disorder Prediction System Using EEG Sensor and Big Data Mining. *Journal of Circuits, Systems and Computers*, 2450197. World Scientific Publishing Company.

[55] Majeed, H. (2020). Watermarking Image Depending on Mojette Transform for Hiding Information. *International Journal Of Computer Sciences And Engineering*, *8*, 8-12.

[56] Mohammed, D., & Omar, M. (2024). Decision Trees Unleashed: Simplifying IoT Malware Detection With Advanced AI Techniques. In *Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology* (pp. 240-258). IGI Global.

[57] Mohammed, D., Omar, M., & Nguyen, V. (2017). Enhancing Cyber Security for Financial Industry through Compliance and Regulatory Standards. In *Security Solutions for Hyperconnectivity and the Internet of Things* (pp. 113-129). IGI Global.

[58] Mohammed, D., Omar, M., & Nguyen, V. (2018). Wireless sensor network security: approaches to detecting and avoiding wormhole attacks. *Journal of Research in Business, Economics and Management*, 10(2), 1860-1864.

[59] Nguyen, V., Mohammed, D., Omar, M., & Banisakher, M. (2018). The Effects of the FCC Net Neutrality Repeal on Security and Privacy. *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)*, 2(2), 21-29. IGI Global.

[60] Nguyen, V., Mohammed, D., Omar, M., & Dean, P. (2020). Net neutrality around the globe: A survey. In *2020 3rd International Conference on Information and Computer Technologies (ICICT)* (pp. 480-488). IEEE.

[61] Nguyen, V., Omar, M., & Mohammed, D. (2017). A Security Framework for Enhancing User Experience. *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)*, 1(1), 19-28. IGI Global.

[62] Omar, M. & Zangana, H. M. (Eds.). (2024). *Redefining Security With Cyber AI*. IGI Global. https://doi.org/10.4018/979-8-3693-6517-5

[63] Omar, M. (2012). *Smartphone Security: Defending Android-based Smartphone Against Emerging Malware Attacks* (Doctoral dissertation, Colorado Technical University).

[64] Omar, M. (2015). Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing. In *Handbook of Research on Security Considerations in Cloud Computing* (pp. 30-38). IGI Global.

[65] Omar, M. (2015). Insider threats: Detecting and controlling malicious insiders. In *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 162-172). IGI Global.

[66] Omar, M. (2019). A world of cyber attacks (a survey).

[67] Omar, M. (2021). Developing Cybersecurity Education Capabilities at Iraqi Universities.

[68] Omar, M. (2021). New insights into database security: An effective and integrated approach for applying access control mechanisms and cryptographic concepts in Microsoft Access environments.

[69] Omar, M. (2022). Application of machine learning (ML) to address cybersecurity threats. In *Machine Learning for Cybersecurity: Innovative Deep Learning Solutions* (pp. 1-11). Springer International Publishing Cham.

[70] Omar, M. (2022). *Machine Learning for Cybersecurity: Innovative Deep Learning Solutions*. Springer Brief. https://link.springer.com/book/978303115

[71] Omar, M. (2022). Malware anomaly detection using local outlier factor technique. In *Machine Learning for Cybersecurity: Innovative Deep Learning Solutions* (pp. 37-48). Springer International Publishing Cham.

[72] Omar, M. (2023). VulDefend: A Novel Technique based on Pattern-exploiting Training for Detecting Software Vulnerabilities Using Language Models. In *2023 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)* (pp. 287-293). IEEE.

[73] Omar, M. (2024). From Attack to Defense: Strengthening DNN Text Classification Against Adversarial Examples. In *Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology* (pp. 174-195). IGI Global.

[74] Omar, M. (2024). Revolutionizing Malware Detection: A Paradigm Shift Through Optimized Convolutional Neural Networks. In *Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology* (pp. 196-220). IGI Global.

[75] Omar, M. (n.d.). *Defending Cyber Systems through Reverse Engineering of Criminal Malware*. Springer Brief. https://link.springer.com/book/9783031116278

[76] Omar, M. (n.d.). Latina Davis Morgan State University 1700 E Cold Spring Ln. Baltimore, MD 21251, USA E-mail: latinaedavis@ hotmail. com.

[77] Omar, M. (n.d.). Machine Learning for Cybersecurity.

[78] Omar, M., & Burrell, D. (2023). From text to threats: A language model approach to software vulnerability detection. *International Journal of Mathematics and Computer in Engineering*.

[79] Omar, M., & Burrell, D. N. (2024). Organizational Dynamics and Bias in Artificial Intelligence (AI) Recruitment Algorithms. In *Evolution of Cross-Sector Cyber Intelligent Markets* (pp. 269-290). IGI Global.

[80] Omar, M., & Dawson, M. (2013). Research in progress-defending android smartphones from malware attacks. In *2013 third international conference on advanced computing and communication technologies (ACCT)* (pp. 288-292). IEEE.

[81] Omar, M., & Mohaisen, D. (2022). Making Adversarially-Trained Language Models Forget with Model Retraining: A Case Study on Hate Speech Detection. In *Companion Proceedings of the Web Conference 2022* (pp. 887-893).

[82] Omar, M., & Shiaeles, S. (2023). VulDetect: A novel technique for detecting software vulnerabilities using Language Models. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE. https://ieeexplore.ieee.org/document/10224924

[83] Omar, M., & Sukthankar, G. (2023). Text-defend: detecting adversarial examples using local outlier factor. In *2023 IEEE 17th international conference on semantic computing (ICSC)* (pp. 118-122). IEEE.

[84] Omar, M., Bauer, R., Fernando, A., Darejeh, A., Rahman, S., Ulusoy, S. K., Arabo, A., Gupta, R., Adedoyin, F., Paul, R. K., & others. (2024). Committee Members. In *Journal of Physics: Conference Series*, 2711, 011001.

[85] Omar, M., Choi, S., Nyang, D., & Mohaisen, D. (2022). Quantifying the performance of adversarial training on language models with distribution shifts. In *Proceedings of the 1st Workshop on Cybersecurity and Social Sciences* (pp. 3-9).

[86] Omar, M., Choi, S., Nyang, D., & Mohaisen, D. (2022). Robust natural language processing: Recent advances, challenges, and future directions. *IEEE Access*, 10, 86038-86056. IEEE.

[87] Omar, M., Gouveia, L. B., Al-Karaki, J., & Mohammed, D. (2022). Reverse-Engineering Malware. In *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security* (pp. 194-217). IGI Global.

[88] Omar, M., Jones, R., Burrell, D. N., Dawson, M., Nobles, C., & Mohammed, D. (2023). Harnessing the power and simplicity of decision trees to detect IoT Malware. In *Transformational Interventions for Business, Technology, and Healthcare* (pp. 215-229). IGI Global.

[89] Omar, M., Mohammed, D., & Nguyen, V. (2017). Defending against malicious insiders: a conceptual framework for predicting, detecting, and deterring malicious insiders. *International Journal of Business Process Integration and Management*, 8(2), 114-119. Inderscience Publishers (IEL).

[90] Omar, M., Mohammed, D., Nguyen, V., Dawson, M., & Banisakher, M. (2021). Android application security. In *Research Anthology on Securing Mobile Technologies and Applications* (pp. 610-625). IGI Global.

[91] Pauu, K. T., Pan, Q., Wu, J., Bashir, A. K., & Omar, M. (2024). IRS-Aided Federated Learning with Dynamic Differential Privacy for UAVs in Emergency Response. *IEEE Internet of Things Magazine*, 7(4), 108-115. IEEE.

[92] Peng, Y., Wang, J., Ye, X., Khan, F., Bashir, A. K., Alshawi, B., Liu, L., & Omar, M. (2024). An intelligent resource allocation strategy with slicing and auction for private edge cloud systems. *Future Generation Computer Systems*, 160, 879-889. North-Holland.

[93] Rajesh, R., Hemalatha, S., Nagarajan, S. M., Devarajan, G. G., Omar, M., & Bashir, A. K. (2024). Threat Detection and Mitigation for Tactile Internet Driven Consumer IoT-Healthcare System. *IEEE Transactions on Consumer Electronics*. IEEE.

[94] Saleem, M. A., Li, X., Mahmood, K., Shamshad, S., Ayub, M. F., & Omar, M. (2023). Provably secure conditional-privacy access control protocol for intelligent customers-centric communication in vanet. *IEEE Transactions on Consumer Electronics*. IEEE.

[95] Sun, Y., Xu, T., Bashir, A. K., Liu, J., & Omar, M. (2023). BcIIS: Blockchain-Based Intelligent Identification Scheme of Massive IoT Devices. In *GLOBECOM 2023-2023 IEEE Global Communications Conference* (pp. 1277-1282). IEEE.

[96] Tao, Y., Wu, J., Pan, Q., Bashir, A. K., & Omar, M. (2024). O-RAN-Based Digital Twin Function Virtualization for Sustainable IoV Service Response: An Asynchronous Hierarchical Reinforcement Learning Approach. *IEEE Transactions on Green Communications and Networking*. IEEE.

[97] Tiwari, N., Ghadi, Y., & Omar, M. (2023). Analysis of Ultrasound Images in Kidney Failure Diagnosis Using Deep Learning. In *Transformational Interventions for Business, Technology, and Healthcare* (pp. 45-74). IGI Global.

[98] Tiwari, N., Omar, M., & Ghadi, Y. (2023). Brain Tumor Classification From Magnetic Resonance Imaging Using Deep Learning and Novel Data Augmentation. In *Transformational Interventions for Business, Technology, and Healthcare* (pp. 392-413). IGI Global.

[99] Umer, M., Aljrees, T., Karamti, H., Ishaq, A., Alsubai, S., Omar, M., Bashir, A. K., & Ashraf, I. (2023). Heart failure patients monitoring using IoT-based remote monitoring system. *Scientific Reports*, 13(1), 19213. Nature Publishing Group UK London.

[100] Wright, J., Dawson Jr, M. E., & Omar, M. (2012). Cyber security and mobile threats: The need for antivirus applications for smartphones. *Journal of Information Systems Technology and Planning*, 5(14), 40-60.

[101] Xu, X., Wu, J., Bashir, A. K., & Omar, M. (2024). Machine Learning and Zero Knowledge Empowered Trustworthy Bitcoin Mixing for Next-G Consumer Electronics Payment. *IEEE Transactions on Consumer Electronics*. IEEE.

[102] Zangana, H. M. (2015). A New Skin Color Based Face Detection Algorithm by Combining Three Color Model Algorithms. *IOSR J. Comput. Eng*, *17*, 06-125.

[103] Zangana, H. M. (2017). A new algorithm for shape detection. *IOSR Journal of Computer Engineering (IOSR-JCE)*, *19*(3), 71-76.

[104] Zangana, H. M. (2017). Library Data Quality Maturity (IIUM as a Case Study). *IOSR-JCE March*, *29*, 2017.

[105] Zangana, H. M. (2017). Watermarking System Using LSB. *IOSR Journal of Computer Engineering*, *19*(3), 75-79.

[106] Zangana, H. M. (2018). Design an information management system for a pharmacy. *International Journal of Advanced Research in Computer and Communication Engineering*, *7*(10).

[107] Zangana, H. M. (2018). Developing Data Warehouse for Student Information System (IIUM as a Case Study). *International Organization of Scientific Research*, *20*(1), 09-14.

[108] Zangana, H. M. (2018). Developing Data Warehouse for Student Information System (IIUM as a Case Study). *International Organization of Scientific Research*, *20*(1), 09-14.

[109] Zangana, H. M. (2018). Implementing a System for Recognizing Optical Characters.

[110] Zangana, H. M. (2019). Issues of Data Management in the Library: A Case Study.

[111] Zangana, H. M. (2019). ITD Data Quality Maturity (A Case Study). *International Journal Of Engineering And Computer Science*, *8*(10).

[112] Zangana, H. M. (2020). Mobile Device Integration in IIUM Service. *International Journal*, *8*(5).

[113] Zangana, H. M. (2021). The Global Finical Crisis from an Islamic Point Of View. *Qubahan Academic Journal*, *1*(2), 55-59.

[114] Zangana, H. M. (2022). Creating a Community-Based Disaster Management System. *Academic Journal of Nawroz University*, *11*(4), 234-244.

[115] Zangana, H. M. (2022). Implementing New Interactive Video Learning System for IIUM. *Academic Journal of Nawroz University*, *11*(2), 23-29.

[116] 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).

[117] Zangana, H. M. (2024). Exploring Blockchain-Based Timestamping Tools: A Comprehensive Review. *Redefining Security With Cyber AI*, 92-110.

[118] Zangana, H. M. (2024). Exploring the Landscape of Website Vulnerability Scanners: A Comprehensive Review and Comparative Analysis. *Redefining Security With Cyber AI*, 111-129.

[119] Zangana, H. M. CHALLENGES AND ISSUES of MANET.

[120] 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.

[121] 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.

[122] 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.

[123] 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).

[124] 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.

[125] Zangana, H. M., & Omar, M. (2020). Threats, Attacks, and Mitigations of Smartphone Security. *Academic Journal of Nawroz University*, *9*(4), 324-332.

[126] Zangana, H. M., & Omar, M. (2020). Threats, Attacks, and Mitigations of Smartphone Security. *Academic Journal of Nawroz University*, 9(4), 324-332.

[127] 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.

[128] 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.

[129] 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.

[130] 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.

[131] 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.

[132] 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.

[133] 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.

[134] 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.

[135] 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).

[136] Zangana, H. M., Natheer Yaseen Ali, & Ayaz khalid Mohammed. (2024). Navigating the Digital Marketplace: A Comprehensive Review of E-Commerce Trends, Challenges, and Innovations. *TIJAB (The International Journal of Applied Business)*, *8*(1), 88–103. https://doi.org/10.20473/tijab.v8.I1.2024.54618

[137] 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.

[138] 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.

[139] 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.

[140] 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.

[141] Zangana, H. M., Tawfiq, N. E., & Omar, M. (2020). Advantages and Challenges of E-Government in Turkey.

[142] Zangana[1], H. M., Tawfiq, N. E., & Omar, M. (2020). Advantages and Challenges of E-Government in Turkey.

[143] 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.

[144] Zhou, S., Ali, A., Al-Fuqaha, A., Omar, M., & Feng, L. (n.d.). Robust Risk-Sensitive Task Offloading for Edge-Enabled Industrial Internet of Things. *IEEE Transactions on Consumer Electronics*