International Journal of Science Academic Research
Vol. 05, Issue 08, pp.8153-8158, August, 2024
Available online at http://www.scienceijsar.com

ISSN: 2582-6425

Research Article

ARTIFICIAL INTELLIGENCE AND BIG DATA ANALYTICS DEVELOPMENTS IN COMBATING CYBERCRIME AND ENHANCING DIGITAL CITIZENSHIP

***Ahmad Abdulqadir Al Rababah**

Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh, Saudi Arabia

Received 20th June 2024; **Accepted** 24th July 2024; **Published online** 30th August 2024

Abstract

Developments in artificial intelligence and big data analytics have significantly contributed to combating cybercrime and enhancing digital citizenship. By using AI technologies such as machine learning and artificial neural networks, large datasets can be analyzed quickly and accurately to detect patterns of fraud and suspicious online activities. For example, AI can be used to identify abnormal behaviors online, such as banking fraud or data breaches, allowing for rapid intervention to prevent crimes before they occur. Additionally, big data analysis can be used to track crime patterns and identify geographic areas at risk of cybercrime, helping to guide development and training efforts for police forces and enhance digital security for citizens. By integrating AI and big data analytics into cybersecurity frameworks, organizations can enhance their ability to detect, prevent, and respond to cyber threats, while also promoting safer and more responsible digital behavior among users. Overall, these technologies work to enhance digital safety and reduce cybercrime, contributing to the promotion of digital citizenship and the creation of a safer and more trustworthy online environment.

Keywords: Digital citizenship, Big data, Cybercrime, Artificial Intelligence, Crimes Detection.

INTRODUCTION

The world today is operating at a rapid pace in the fields of artificial intelligence and big data analytics, and this technological advancement is closely linked to combating cybercrime and enhancing digital citizenship. From this standpoint, attention is directed towards conferences in this field, which are considered vital tools for promoting collaboration in combating cybercrime and enhancing digital citizenship. These conferences also provide essential opportunities for sharing knowledge and experiences in this crucial area. This field is particularly important in an era where cybercrime has increased and continuously evolved. Researchers and innovators aim to employ AI technology to reduce this harmful phenomenon and work to stop criminal activities online. Due to the increasing electronic threats, these innovative technologies contribute to providing effective solutions to address online security threats, enhance trust in digital transactions, and provide comprehensive online security protection. Through the use of big data analytics, organizations can gather and analyze vast amounts of data from multiple sources to uncover new trends and patterns in the behavior of cybercriminals. These technologies can also be used to improve data security and ensure the safety of personal information online. Additionally, AI can help enhance digital citizenship by providing tools and technologies that help individuals stay safe online and understand how to protect their privacy and personal information on the web. AI-developed technology spans a wide range of fields such as medicine, agriculture, manufacturing, and even education. Thanks to AI, we see improvements in diagnosing complex diseases, increased agricultural crop productivity, reduced waste in manufacturing processes, and personalized education to meet the needs of each student in particular. Furthermore, AI contributes to enhancing security and simplifying daily operations in general.

Corresponding Author:** ***Ahmad Abdulqadir Al Rababah,
Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh, Saudi Arabia.

ANALYSIS AND DISCUSSION

Advancements in artificial intelligence play a crucial role in combating cybercrime and enhancing digital citizenship through data analysis and pattern recognition. AI is utilized to analyze the increasing volumes of big data related to cybercrime, thereby identifying potential patterns and trends, automating verification processes, and detecting fraud. AI also aids in developing fraud detection systems capable of identifying illicit online activities, whether related to electronic forgery, data breaches, or identity theft. Additionally, machine learning and intelligent interaction as part of AI techniques contribute to data analysis and improve performance over time. This means better capability in detecting unusual behaviors and effectively addressing new threats (Figure 1).

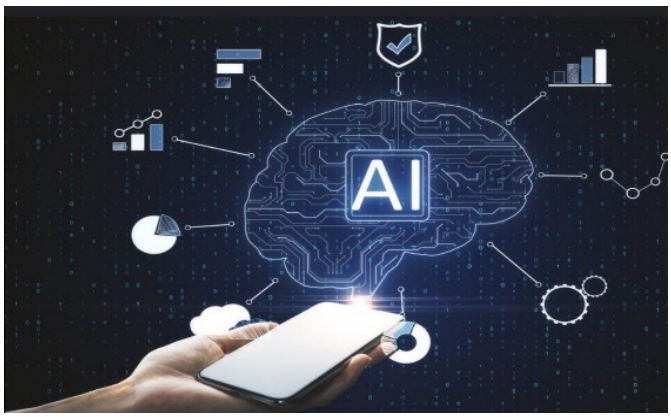

Figure 1. Areas of Artificial Intelligence Applications

Enhancing cybersecurity awareness and digital literacy enables experts to use artificial intelligence to develop security awareness tools and provide digital training to citizens, thereby increasing their awareness of electronic risks and preventive measures. Therefore, human-computer interaction in criminal investigations utilizes AI techniques, which can support investigators in gathering and analyzing evidence more

effectively, providing detailed reports and data-driven analyses in general. Additionally, artificial intelligence represents a significant advancement in the field of combating cybercrime, enhancing individuals' and institutions' ability to counter digital security threats and promote digital citizenship (Figure 2).

Figure 2. Human-Machine Interaction

RESEARCH METHODOLOGY

Methods and Procedures for Using Artificial Intelligence and Big Data Analytics in Combating Cybercrime and Enhancing Digital Citizenship:

- **Detecting New Threats:** Cybercrimes constantly evolve, necessitating readiness for emerging threats. Using big data analytics, large datasets from previous activities can be analyzed to detect new and unusual patterns indicating potential threats. This allows organizations to take early preventive actions and strengthen their security systems.
- **Identity Verification and Counterfeit Prevention:** Artificial intelligence techniques can verify digital identities of individuals and entities by analyzing user behavior, personal data, and facial recognition information to ensure the claimed identity matches the actual person. This reduces the risk of electronic forgery and fraud, thereby enhancing digital citizenship.
- **Predictive Crime Analysis:** Artificial intelligence and big data analytics can analyze criminal data and other digital information to identify new crime trends and patterns.
- **Real-Time Response and Analysis:** AI and big data analytics operate at high speeds, enabling real-time analysis and response to security threats. Potential activities related to cybercrimes can be monitored and addressed promptly, reducing potential damage and enhancing digital security.
- **Assistance in Criminal Investigations:** AI and big data analytics can assist in processing and analyzing large volumes of data efficiently, aiding in criminal investigations.
- **Development of Technologies and Algorithms:** Advancements in AI and data analytics require the development of advanced technologies and algorithms capable of processing vast amounts of data quickly and efficiently, such as machine learning techniques and artificial neural networks.
- **Scientific Research and Practical Applications:** Continuous scientific research is essential to better understand these technologies and their practical applications across various fields like medicine, marketing, education, security, and others.
- **Ensuring Sufficient Data:** Adequate and diverse digital data is crucial for training AI models and developing data analytics systems. Therefore, companies and institutions need to effectively collect and securely store data for maximum utilization.
- **Education and Training:** Opportunities for education and training in AI and data analytics should be provided to professionals, researchers, and students to empower them with the necessary skills for effective and creative use of these technologies.
- **Effective Policies and Regulations:** Progress in AI, data analytics, and enhancing digital citizenship requires effective policies and regulations that define the legal and ethical frameworks for responsible and secure use of these technologies.
- **Digital Awareness and Education:** Increasing awareness and education about AI, data analytics, and digital user rights are crucial for enabling individuals to understand the potential impacts and benefits of these technologies and engage effectively in the digital community.

Implementing these comprehensive methods and procedures can achieve sustainable development in AI and enhance digital citizenship, contributing to improving daily life for people and advancing societies economically and socially.

Summary and recommendations

Based on the methods and procedures discussed for using artificial intelligence and big data analytics in combating cybercrime and enhancing digital citizenship, here are some conclusions and recommendations:

- **Directing Security Efforts:** Artificial intelligence can be used to identify new patterns of cybercrimes and direct security and investigative efforts more effectively to combat these emerging threats.
- **Enhancing International Cooperation:** Big data analytics enhances cooperation between countries and entities involved in combating cybercrimes, facilitating the exchange of information and expertise to collectively address cyber threats.
- **Raising Awareness and Education:** AI and big data analytics can be used to understand online infiltrators and fraudsters' behaviors, improving awareness and education programs for citizens about the risks of cybercrimes and preventive measures.
- **Improving Prediction and Prevention:** AI and data analytics can predict potential cybercrimes and take appropriate preventive actions, thereby enhancing digital security for citizens and organizations.
- **Enhancing Emergency Response:** AI and data analytics can improve emergency response by security agencies to cyber emergencies, minimizing damages and facilitating quick system recovery.
- **Deeper and Comprehensive Analysis:** AI and big data analytics enable detailed and comprehensive analysis of vast amounts of data, helping better understand patterns, trends, and influencing factors in cybercrimes.
- **Reinforcing Digital Governance:** Effective data analysis methods and smart technology deployment reinforce digital governance across various sectors and institutions, fostering a digital environment characterized by transparency and accountability. This enhances trust in the secure use of digital technology and reduces cybercrime threats.

Based on these points, it can be concluded that advancements in artificial intelligence and big data analytics are crucial tools in combating cybercrimes and enhancing digital citizenship. These powerful and effective technologies should be used wisely and responsibly to maximize societal benefits. As artificial intelligence and big data analytics continue to advance in combating cybercrime and enhancing digital citizenship, there are a number of recommendations, including:

- Information Exchange and International Cooperation: Enhanced cooperation between countries is essential for sharing information and expertise in combating cybercrime. International mechanisms should be established for data analysis and exchange of information on cyber threats and effective methods to combat them.
- Citizen Awareness and Encouraging Reporting: Efforts should be intensified to raise awareness among citizens about the risks of cybercrime and how to protect themselves, as well as encouraging them to report fraud and illicit online activities they encounter.
- Enhancing Digital Investigations: Technical and training capabilities of digital investigators should be strengthened to analyze digital data effectively and legally. Legal and technical procedures for using digital evidence in courts should also be developed and improved.
- Focus on Training and Education: Specialized training programs should be developed for investigators and cybersecurity professionals to enhance their capabilities in using modern technologies to combat cybercrime.
- Using Technology for Criminal Investigation: Artificial intelligence and big data analytics should be used to analyze digital evidence and identify perpetrators, facilitated by developing tools and software that streamline data collection and analysis.
- Enhancing Transparency and Accountability: Transparency and accountability in cybercrime prevention efforts should be reinforced, including providing regular reports on successes, challenges, and failures in this field, and clearly defining responsibilities.

Efforts to combat cybercrime and enhance digital citizenship can be effectively and sustainably strengthened. By maximizing these recommendations and technological advancements, efforts to combat cybercrime can be enhanced and authorities' response to these increasing challenges can be improved. Through enhancing international cooperation, sharing knowledge, and expertise, capabilities to combat cybercrime can be strengthened globally. Legislations and policies should also be considered to address new challenges in the digital crime world, with a focus on protecting individuals' rights and preserving personal freedoms. Through this comprehensive approach, a safer and more trusted environment can be built in the digital world, enhancing economic and social development globally. In the current technological age, our world is witnessing tremendous transformations in the field of artificial intelligence, reflecting rapid developments in how we interact with technology. Emerging technology plays a vital role in various aspects of our lives, opening up possibilities we could only dream of before, enabling us to enhance productivity and significantly improve our lives.

The most significant outcomes of advancements in artificial intelligence and big data analytics in combating crimes and enhancing digital citizenship are:

Early Detection of Crimes

It refers to the process of identifying criminal activities or intentions at an early stage, ideally before they escalate into more serious offenses or cause significant harm. This concept often involves the use of proactive measures, such as surveillance, data analysis, and predictive algorithms, to spot suspicious behaviors or patterns that could indicate criminal activity. Early detection aims to enable timely intervention and prevention efforts, thereby reducing the impact and frequency of criminal incidents. Here are some key aspects involved in the early detection of crimes:

- Analyzing user behavior online to identify suspicious patterns that may indicate criminal activity, such as: - Repeated attempts to log into user accounts. - Downloading suspicious files. - Visiting malicious websites.
- Using machine learning techniques to monitor and detect abnormal activities in real-time.
- Analyzing data from various sources, such as: - Network logs. - Financial transaction records. - Social media platforms.
- Using natural language processing techniques to analyze texts and identify harmful content.
- Rapid Response in: - Real-time data analysis to identify and prevent electronic attacks before they occur. - Using artificial intelligence techniques to identify weaknesses in cybersecurity systems and provide recommendations for improvement. - Sending immediate alerts to relevant authorities when any suspicious activity occurs.
- Investigation Through: - Assisting investigators in linking evidence and identifying criminals. - Analyzing big data to establish links between various criminal activities. - Using facial recognition and fingerprinting technologies to identify suspects. - Using data analysis techniques to recover deleted or hidden data.
- Securing Prevention: - Enhancing cybersecurity systems and developing new tools for preventing cybercrimes. - Using artificial intelligence to identify emerging threats and provide recommendations to protect information systems. - Raising awareness about the risks of cybercrimes and how to protect oneself.

Enhancing Digital Citizenship

It refers to the process of improving individuals' understanding, behavior, and responsibilities in the digital world. Digital citizenship involves the ethical and responsible use of technology and the internet, emphasizing safe, respectful, and informed interactions online. Here are some key aspects involved in enhancing digital citizenship:

- **Education and Awareness**: Teaching individuals, especially young people, about the rights, responsibilities, and risks associated with being online. This includes understanding privacy, data protection, and the ethical use of digital content.
- **Critical Thinking and Media Literacy**: Encouraging users to critically evaluate the information they encounter online, recognize misinformation, and differentiate between reliable and unreliable sources.
- **Online Etiquette and Communication**: Promoting respectful and constructive communication in digital spaces, including social media, forums, and other online

communities. This also involves understanding the impact of one's online behavior on others.

- **Cybersecurity Practices**: Educating individuals on how to protect themselves from online threats, such as phishing, hacking, and identity theft. This includes using strong passwords, recognizing scams, and safeguarding personal information.
- **Digital Footprint Management**: Helping users understand the long-term implications of their online actions and how to manage their digital footprint, including the content they post and the interactions they engage in.
- **Inclusivity and Accessibility**: Ensuring that digital platforms are inclusive and accessible to all users, regardless of their abilities or backgrounds. This includes promoting diversity and preventing online discrimination and harassment.
- **Empathy and Cultural Sensitivity**: Encouraging users to be empathetic and culturally sensitive in their online interactions, recognizing and respecting diverse perspectives and experiences.

By enhancing digital citizenship, individuals can contribute to a safer, more inclusive, and ethical online environment, fostering positive digital communities and reducing harmful online behaviors.

Examples of AI and Big Data Applications in Combating Cybercrimes:

- **"Etimad" System**: An artificial intelligence system developed by the Saudi Ministry of Interior to detect and prevent cybercrimes. The system can identify suspicious activities in real-time and provide alerts to relevant authorities.
- **"Cyber Storm" Platform:** A big data analytics platform developed by the European Union for combating cybercrimes. The platform aims to provide a secure environment for exchanging information and expertise among various stakeholders involved in combating cybercrimes.
- **IBM Watson for Cyber Security**: IBM Watson uses AI to analyze vast amounts of security data, helping organizations identify and respond to cyber threats more effectively. It can detect patterns in cyberattacks and provide insights to enhance cybersecurity measures.
- **Darktrace**: Darktrace utilizes AI and machine learning to detect and respond to cyber threats in real-time. It employs behavioral analytics to identify abnormal network activities that may indicate potential cyber attacks.
- **Splunk Enterprise Security**: Splunk Enterprise Security utilizes big data analytics to provide a centralized platform for monitoring, detecting, and responding to cybersecurity threats. It aggregates and analyzes data from various sources to detect anomalies and potential security incidents.
- **FireEye Helix**: Fire Eye Helix leverages AI-powered analytics to automate threat detection and response. It integrates with FireEye's threat intelligence to provide real-time insights into emerging cyber threats and helps organizations mitigate risks effectively.
- **Cisco Stealth watch**: Cisco Stealth watch uses AI-driven analytics to monitor network traffic and detect anomalies that may indicate malicious activities. It provides visibility into the entire network and helps organizations respond to cyber threats promptly.

These examples illustrate how AI and Big Data technologies are employed across different platforms and solutions to enhance cybersecurity efforts and combat cybercrimes effectively.

Conclusion

The evolution of technology considers the use of big data by both public and private entities in combating cybercrime a crucial step in addressing increasing digital threats. By utilizing artificial intelligence techniques such as machine learning and artificial neural networks, it becomes possible to analyze big data quickly and accurately, surpassing human capabilities. This aids in detecting patterns of cybercrime, predicting potential cyber attacks, and enhancing cybersecurity overall. Governments, companies, and tech institutions adopting AI and big data analytics technologies can continuously enhance digital citizenship and protection from online threats. Students can play a vital role in effectively developing and applying these technologies and applications to combat cybercrime. It's imperative to emphasize the importance of deep learning and training in using AI and big data analytics to tackle current and future digital challenges. Additionally, students should be aware of privacy legislation and cybersecurity to achieve a balance between digital security and individual rights. Internet crimes are an increasing phenomenon that requires vigilance and electronic awareness. Through awareness and the enhancement of electronic protection, we can reduce the risk of falling victim to these crimes and protect our data and personal information. By following these trends and practices, students will play a pivotal role in promoting digital citizenship and protecting personal data, thereby contributing to the building of safe and prosperous digital communities. In conclusion, understanding the nature of cybercrimes is essential for protecting individuals and institutions from growing digital threats. We all must work together to raise awareness and implement the necessary security measures to minimize the impact of these crimes on our digital lives.

REFERENCES

1. Cao, Duc M., et al. "Advanced cybercrime detection: A comprehensive study on supervised and unsupervised machine learning approaches using real-world datasets." *Journal of Computer Science and Technology Studies,* 6.1 (2024): 40-48.
2. Ahmad Al Rababah, "Implementation of Software Systems Packages in Visual Internal Structures", *Journal of Theoretical and Applied Information Technology,* Volume 95, Issue 19 (2017), Pages: 5237-5244.
3. Chintalapati, Shireesha, and M.V. Raghunadh. "Automated attendance management system based on face recognition algorithms." *International Conference on Computational Intelligence and Computing Research. IEEE,* 2015.
4. Pangrazio, Luci, and Julian Sefton-Green. "Digital rights, digital citizenship and digital literacy: What's the difference?" *Journal of new approaches in educational research*, 10.1 (2021): 15-27.
5. Ahmad AlRababah "Implementations of Hybrid FPGA Microwave Format Extension as a Control Device", *IJCSNS International Journal of Computer Science and Network Security,* VOL.18 No.11, November 2018.

6. Jha, Abhishek. "Classroom attendance system using facial recognition system." *The International Journal of Mathematics, Science, Technology and Management,* 2014.
7. Taherdoost, Hamed. "Insights into Cybercrime Detection and Response: A Review of Time Factor." *Information* 15.5 (2024): 273.
8. Ahmad AlRababah "Watermarking implementation on digital images and electronic signatures", *International Journal of Advanced and Applied Sciences,* Volume 4, Issue 10 (October 2017), Pages: 160-164.
9. Riya, G. Lakshmi, et al. "Implementation of attendance management system using SMART-FR." *International Journal of Advance Research Computer and Communication Engineering,* 2015.
10. Chen, Laure Lu, et al. "Conceptualization and measurement of digital citizenship across disciplines." *Educational Research Review* 33 (2021): 100379.
11. Ahmad Al Rababah. "A New Model of Information Systems Efficiency based on Key Performance Indicator (KPI)" *(IJACSA) International Journal of Advanced Computer Science and Applications,* Vol. 8, No. 3, 2017.
12. Akash G, Rupali B and Shobhana S. "SDLC (Software Development Life Cycle)". Published 2014. https://www.slideshare.net/akash250690/sdlc-models-38873234.
13. Al Rababah A. A., "Neural networks precision in technical vision sys-tems," *IJCSNS*, vol. 20, no. 3, p. 29, 2020.
14. Gajjar, Vishalkumar Ravindrakumar, and Hamed Taherdoost. "Cybercrime on a Global Scale: Trends, Policies, and Cybersecurity Strategies." *2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*. IEEE, 2024.
15. Simonyan K. and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," arXiv preprint arXiv:1409.1556, 2014.
16. M. Yousef, K. F. Hussain, and U. S. Mohammed, "Accurate, data-efficient, unconstrained text recognition with convolutional neural net-works," *Pattern Recognition,* vol. 108, p. 107482, 2020.
17. Öztürk, Gülcan. "Digital citizenship and its teaching: A literature review." *Journal of Educational Technology and Online Learning* 4.1 (2021): 31-45.
18. Israa Al-Barazanchi, Aparna Murthy, Ahmad Abdul Qadir Al Rababah, Ghadeer Khader, Haider Rasheed Abdulshaheed, Hafiz Tayyab Rauf, Elika Daghighi, Yitong Niu. "Blockchain Technology - Based Solutions for IOT Security" *IJCSM : Iraqi Journal for Computer Science and Mathematics*, vol. 3, no. 1, Jan. 2022
19. L. Biewald, "Experiment tracking with weights and biases," 2020, software available from wandb.com. [Online]. Available: https://www.wandb.com
20. Ahmad AlRababah "Assurance Quality and Efficiency in Corporate Information Systems", *IJCSNS International Journal of Computer Science and Network Security,* VOL.19 No.4, April 2019.
21. Gumma, Yalamandeswara Rao, and Subbarao Peram. "Review of Cybercrime Detection Approaches using Machine Learning and Deep Learning Techniques." *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*. IEEE, 2024.
22. Jayalakshmi T. and A. Santhakumaran, "Statistical normalization and back propagation for classification," *International Journal of Computer Theory and Engineering,* vol. 3, no. 1, pp. 1793– 8201, 2011.
23. Ruenphongphun, Prarichart, Aukkapong Sukkamart, and Paitoon Pimdee. "Thai Undergraduate Digital Citizenship Skills Education: A Second-Order Confirmatory Factor Analysis." *World Journal on Educational Technology: Current Issues* 13.3 (2021): 370-385.
24. Ahmad Al Rababah "Problems Solving of Cell Subscribers based on Expert Systems Neural Networks" *International Journal of Advanced Computer Science and Applications (IJACSA),* 10(12), 2019.
25. Kim, Yongyeon, Byung-Won On, and Ingyu Lee. "Two-step Automated Cybercrime Coded Word Detection using Multi-level Representation Learning." *arXiv preprint arXiv: 2403.10838* (2024).
26. He K., X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 770–778.
27. Hochreiter S. and J. Schmidhuber, "Long short- term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.
28. Ahmad Al Rababah, "Digital image encryption implementations based on aes algorithm", *Vawkum Transactions on Computer Sciences,* Volume 13, Number 1, May-June , 2017, Pages: 1-9.
29. Pedrycz, Witold. Granular computing: analysis and design of intelligent systems. CRC press. Published 2018.
30. Reema Mrayyan, Ahmad AlRababah, "Debugging of Parallel Programs using Distributed Cooperating Components". *IJCSNS International Journal of Computer Science and Network Security,* VOL.21 No.12, December 2021.
31. Kassa, Yidnekachew Worku, Joshua Isaac James, and Elefelious Getachew Belay. "Cybercrime Intention Recognition: A Systematic Literature Review." *Information* 15.5 (2024): 263.
32. Antoniou, Andreas. Digital filters: analysis, design, and signal processing applications. McGraw-Hill Education. Published 2018
33. Ahmad Al Rababah, "Neural Networks Precision in Technical Vision Systems" *IJCSNS International Journal of Computer Science and Network Security,* VOL.20 No.3, March 2020.
34. Atakishiyev, Shahin, et al. "A multi-component framework for the analysis and design of explainable artificial intelligence." Published 2020.
35. Vishal, " Python SQLite tutorial using sqlite3" Updated in 2021.
36. Al-Sai, Zaher Ali, et al. "Explore big data analytics applications and opportunities: A review." *Big Data and Cognitive Computing* 6.4 (2022): 157.
37. Ahmad Al Rababah, Ahmad Alzahrani. "Software Maintenance Model through the Development Distinct Stages", *IJCSNS International Journal of Computer Science and Network Security,* VOL.19 No.2, February 2019.
38. Thomas Hamilton, "What is Software Testing? Definition, Basics & Types in Software Engineering". Published 2021.
39. Lalbihari Barik, Ahmad AbdulQadir AlRababah, Yasser Difulah Al-Otaibi. "Enhancing Educational Data Mining based ICT Competency among e- Learning Tutors using Statistical Classifier" *International Journal of Advanced Computer Science and Applications (IJACSA),* Volume 11 Issue 3 March 2020.

40. Al-Sai, Zaher Ali, et al. "Explore big data analytics applications and opportunities: A review." *Big Data and Cognitive Computing* 6.4 (2022): 157.
41. Ahmad AlRababah, Bandar Ali Alghamdi. "Information Protection Method in Distributed Computer Networks Based on Routing Algorithms" *IJCSNS International Journal of Computer Science and Network Security,* VOL.19 No.2, February 2019.
42. Shukla, Ratnesh Kumar, and Arvind Kumar Tiwari. "Security Analysis of the Cyber Crime." *The Ethical Frontier of AI and Data Analysis*. IGI Global, 2024. 257-271.
43. Patil, Rachana Y., et al. "Proactive cyber defense through a comprehensive forensic layer for cybercrime attribution." *International Journal of Information Technology* (2024): 1-18.
44. Meshram, Bandu B., and Manish Kumar Singh. "Cyberguard: Cybercrime Risk Management And Insurance, Compensation, Punishment Model In The Digital Realm." *Educational Administration: Theory and Practice* 30.6 (2024): 4294-4322.
45. Ahmad Al Rababah. "Data Flows Management and Control in Computer Networks", *(IJACSA) International Journal of Advanced Computer Science and Applications,* Vol. 9, No. 11, 2018.
46. Yin, Yunqiang, et al. "Big data analytics in production and distribution management." *International Journal of Production Research* 60.22 (2022): 6682-6690.
47. Jujjuri, RamaDevi, et al. "Detection of cyber crime based on facial pattern enhancement using machine learning and image processing techniques." *Using computational intelligence for the dark web and illicit behavior detection*. IGI Global, 2022. 150-165.
48. Dahiya, Rajiv, et al. "Big data analytics and competitive advantage: the strategic role of firm-specific knowledge." *Journal of Strategy and Management* 15.2 (2022): 175-193.
49. Ahmad Al Rababah. "On the associative memory utilization in English- Arabic natural language processing", *International Journal of Advanced and Applied Sciences,* Volume 4, Issue 8 (August 2017), Pages: 14-18. Top of Form.
50. Mahajan, Shilpa, Mehak Khurana, and Vania Vieira Estrela, eds. *Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection*. John Wiley & Sons, 2024.
51. Abdulrahman, Mayasa M., et al. "Innovative Progress in Phased-Array Antenna Systems for Ultra-Low Latency and High-Speed Communication Networks for Resilient Infrastructure." Mathematical Modelling of Engineering Problems 11.7 (2024).
52. Dhashanamoorthi, Balaji. "Analyzing detection algorithms for cybersecurity in financial institutions." *International Journal of Science and Research Archive* 11.2 (2024): 558-568.
53. Cheng, Jie, et al. "The impact of business intelligence, big data analytics capability, and green knowledge management on sustainability performance." *Journal of Cleaner Production* 429 (2023): 139410.
54. Lungu, Nelson, et al. "NIST CSF-2.0 Compliant GPU Shader Execution." *Engineering, Technology & Applied Science Research* 14.4 (2024): 15187-15193.
55. Cheng, Jie, et al. "The impact of business intelligence, big data analytics capability, and green knowledge management on sustainability performance." *Journal of Cleaner Production* 429 (2023): 139410.
56. Al Rababah, Ahmad AbdulQadir. "Assessing the Effectiveness of UML Models in Software System Development."

****