The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 2 | February 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

The Impact of Artificial Intelligence on Cyber Security and Education System

[1]Tilak Kumar Rathour, [2]Raj Kumar Singh, [3]Aaryan Rastogi

[1, 2,3]Assistant Professor

[1, 2,3]Department of Computer Application

[1, 2,3]Future University, Bareilly, UP, India

ARTICLE DETAILS

Research Paper

Accepted: 28-02-2025

Published: 14-03-2025

Keywords:

Artificial Intelligence, Cyber Security, Cyber Threats, Education System, powerful tools

ABSTRACT

In this study discussed about the impact of artificial intelligence (AI) on cyber security (CS) and education system (ES). In the modern time the AI is very powerful tool for cyber security, education, threats, and many others. In the present time cyber crime rate is very high like as an online threats, cyber-attack, and improve incident. In this study also discussed about the role of AI in cyber security, the emergence of AI in cyber security, application of AI for cyber security, benefits of AI in cyber security and future aspects, and disadvantages of AI in security. In this study also discussed about the impact of AI on education system & student's brain.

DOI : https://doi.org/10.5281/zenodo.15030608

Introduction

Artificial intelligence (AI) refers to the development of computer systems that can perform tasks that typically require human intelligence, such as learning, problem-solving, decision-making, and perception. Design to perform a specific task, such as facial recognition, language translation, or playing chess this phenomenon is called narrow or weak AI. Aims to perform any intellectual task that a human can possessing human-like intelligence, reasoning, and problem-solving abilities, this phenomenon is called general or strong AI. Significantly surpasses human intelligence, potentially leading to

exponential growth in technological advancements this phenomenon is called superintelligence. Key point of artificial intelligence technologies defined as machine learning (ML), deep learning (DL), natural language processing (NLP), and computer vision. Applications of artificial intelligence defined as virtual assistants, image and speech recognition, predictive maintenance, and autonomous vehicles. Benefits of artificial intelligence defined as increased efficiency, improved accuracy, enhance customer experience, and innovation and competitiveness. Challenges and concerns of artificial intelligence defined as job displacement, bias and fairness, security and privacy, and ethics and accountability. Positive impacts of AI on cybersecurity defined as enhanced threat detection, improved incident response, predictive analytics, and increased efficiency. Negative impacts of AI on cybersecurity defined as adversarial attacks, AI-powered malware, data poisoning, and increased complexity. Artificial intelligence powered cybersecurity solutions defined as AI-powered firewalls, AI-powered endpoint detection and response, and AI-powered security information and event management (SIEM) systems. Future of AI in cybersecurity defined as increased adoption, improved accuracy, increased automation, and new threats and challenges. Positive impacts of artificial intelligence on education defined as personalized learning, intelligent tutoring systems, automated grading, and enhanced accessibility and data-driven insights. Negative impacts of AI on education defined as job displacement, depersonalization, bias and inequity, technical issues, and lack of transparency. Artificial intelligence powered educational tools defined as adaptive learning platforms, intelligence tutorial systems, virtual learning environments, and natural language processing tools. Future of artificial intelligence in education defined as increased adoption, improved accessibility, enhanced teacher support, and new forms of assessment.

Literature review

After study of some research paper & articles then find that some authors discussed different types of theories which are based on cyber threats, cyber crime, and online fraud. In the present time the utilization artificial intelligence is very huge some areas mention here like as a banking sector, education sector, manufacturing industries, software industries and many others these all are based on artificial intelligence technologies. Before some time, maximum organisation does the work based on the manually no work by using software. Due to this reason every organization has need of more manpower. Now discussed about the education areas before some time no smart class was not available in the classroom. In the present time many tools are available in the market which is help to learn the education. For examples; - ChatGPT, Meta AI, Google Classroom, Canvas, Blackboard, and many

others & Intelligent Tutoring systems defined as DreamBox, Carnegie Learning's Cognitive Tutor, and Knewton. Natural Language Processing Tools defined as Grammarly, Turnitin, and Language Tool. Artificial intelligence powered assessment tools defined as ProctorU, Kryterion, and AssessFirst. Artificial intelligence powered learning platforms defined as Coursera, Udemy, and edX.

Applications of artificial intelligence

In modern time very huge utilization of artificial intelligence in the different areas some areas mention here like as a healthcare, personalization medicine, virtual nursing assistance and many others. Applications of AI in the education system defined as intelligent tutorial systems, automated grading, virtual learning environments. Applications of AI in the finance sector defined as risk management, fraud detection, and personalized financial planning. Applications of AI in transportation sector defined as autonomous, predictive maintenance, route optimization. Application of AI in the cybersecurity defined as threat detection, incident response, and vulnerability management.

Advantages of artificial intelligence

In the present time more utilization of artificial intelligence for enhance the learning capacity, storage system, enhance the software development some advantages of artificial intelligence mention here like as improved efficiency; - automation, speed. Advantages of artificial intelligence in the enhanced accuracy defined as precision, consistency. Advantages of AI in the improved decision-making defined as data analysis, predictive analytics. Advantages of enhanced customer experience defined as personalization, Chatbots. Advantages of innovation and competitiveness defined as new business models, competitive advantage. Advantages of improved healthcare defined as medical diagnosis, personalized medicine. Advantages of artificial intelligence in environmental benefits defined as energy efficiency, sustainability.

Disadvantages of artificial intelligence

In this time many drawbacks of artificial intelligence defined as job displacement in this area has automation, unemployment. Drawback of artificial intelligence in the bias and discrimination defined as data bias, lack of transparency. Disadvantages of artificial intelligence in the security risk defined as cyber attacks, adversarial attacks. Disadvantages of artificial intelligence in dependence on data defined as data quality, data availability. Lack of human judgement & emotional intelligence defined as contextual understanding, AI systems may struggle to understand the nuances of human language and

behaviour, leading to misinterpretation. Regulatory challenges & environmental impact defined as lack of regulation, emotional intelligence, energy consumption, E-waste.

Role of AI in Cyber Security

Artificial intelligence (AI) plays a crucial role in cybersecurity, enhancing threat detection, incident response, and predicative analytics. Benefits of artificial intelligence in cybersecurity defined as improved threat detection, enhanced incident response, predictive analytics, and increased efficiency. The application of AI in cybersecurity defined as anomaly detection, malware detection, and phishing detection, vulnerability management. Artificial intelligence powered cybersecurity solutions defined as machine learning-based intrusion detection systems, artificial intelligence security information and event management (SIEM) systems, artificial intelligence powered endpoint detection and response, and artificial intelligence powered incident response platforms. Challenges and limitations of artificial intelligence in the cybersecurity defined as adversarial attacks, bias and inequity, technical issues, lack of transparency and explainability. Future of artificial intelligence in the cybersecurity defined as increased adoption, improved transparency and explainability, and addressing bias and inequity.

Role of AI in the education

In the present time, very huge utilization of artificial intelligence in the education system for enhances the learning capacity of students. Artificial intelligence (AI) is transforming the education sector in various ways defined as personalized learning, automated grading, enhanced accessibility, data driven insights, intelligent assessment systems, virtual teaching assistants, limitation and challenges. Role of personalized in the education system defined as adaptive learning, intelligent tutoring systems. Role of automated grading in the education system defined as efficient grading, accurate grading and enhanced accessibility defined as virtual learning environments, natural language processing. Data driven insights in the education system defined as predictive analytics, learning analytics. Intelligent assessment systems in the education system defined as automated assessment, adaptive assessment. Virtual teaching assistants in the education system defined as artificial intelligent powered TAs, personalized support. Limitations and challenges defined as bias and inequity, technical issues, and dependence on data.

The emergence of artificial intelligence in cybersecurity

Cybersecurity has very important role to prevent cyber threats, organization detection and save from online fraud. The benefits of artificial intelligence in cybersecurity defined as improved threat detection,

enhanced incident response, predictive analytics, and increased efficiency. Application of artificial intelligence in the cybersecurity defined as anomaly detections, malware detection, phishing detection, vulnerability management. Artificial intelligence powered cybersecurity solutions defined as machine learning-based intrusion detection systems, artificial intelligence powered security information and event management systems, artificial intelligence powered endpoint detection and response, and artificial intelligence powered incident response platforms. Challenges and limitation of artificial intelligence in the cybersecurity defined as adversarial attacks, bias and inequity, technical issues, and lack of transparency and explain ability.

The emergence of artificial intelligence (AI) in the education system

Artificial intelligence provide a new era in the education system & artificial intelligence have more advance feature due to this the education is more advance. Online education is possible by using artificial intelligence. By using artificial intelligence to solve student's problems & enhance the learning capacity. In the present time, smart board is available in the student's classroom due to try to understand of students by tutor become very easy. The artificial intelligence has more advance features which is more powerful to enhance the education system. The artificial intelligence (AI) is very important role in the research and development (R&D). The artificial intelligence is more advanced features due to this in the present time manufacturing industries, education industries, and software industries is in the growing condition due to this reason the artificial intelligence is more effective on the education.

Future aspects of artificial intelligence in the cybersecurity and education system

Artificial intelligence powered security solutions will become more widespread, enabling more effective and effective cybersecurity operations. Artificial intelligence powered systems will become more adept at detecting and responding to cyber threats in the real-time. Artificial intelligence powered systems will become more effective at predicting potential cyber threats, enabling proactive measures to prevent them & cybersecurity will become more effective at predicting potential cyber threats, enabling proactive measures to prevent them. Artificial intelligence powered cybersecurity solution will prioritize explain ability and transparency, enabling cybersecurity professionals to understand AI driven decision making processes. Future aspects of artificial intelligence in the education system defined as artificial intelligence powered systems will create personalized learning experiences tailored to individual students needs, abilities, and learning styles. Artificial intelligence powered system will provide personalized cybersecurity education and training, enhancing cybersecurity awareness and literacy. And

AI will provide cybersecurity solution specifically designed for AI powered education, protecting against AI cyber threats.

Conclusion

Artificial intelligence has very important role in the cybersecurity and education system. Enhancing the learning capacity of students in possible by using artificial intelligence. To stop the online fraud is possible by artificial intelligence. To provide the web security and to stop cyber attack on the banking sector, education sector, health sector, and many others. In this study find that the artificial intelligence is more effective on the cybersecurity and education sector because in the modern time is available very easy way of learning platform due to this it's very useful for students. To solve the problems of students like as assignment, tutorial and many others and due to AI's tools very attractive content is available in the market which is very useful for student.

References

1. Ishaq Azhar Mohammed, "artificial intelligence for cybersecurity: a systematic mapping of literature", international journal of innovations in engineering research and technology [IJIERT], volume 7, issue 9, sep.-2020, ISSN: 2394-3696.
2. Rajneesh Kumar, "Artificial Intelligence: A Path to Innovation", International Journal of Scientific Research in Science and Technology (IJSRST), 2017 IJSRST | Volume 3 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X.
3. Generative AI for Cyber Security: Analyzing the Potential of ChatGPT, DALL-E, and Other Models for Enhancing the Security Space. Authors: Siva Sai; Utkarsh Yashvardhan; Vinay Chamola; Biplab Sikdar.
4. Impact of Artificial Intelligence on Information Security in Business. Authors: Safiya Ahmed Alawadhi; Areej Zowayed; Hamad Abdulla; Moaiad Ahmad Khder; Basel J. A. Ali
5. Cyber Security Issues and Challenges Related to Generative AI and ChatGPT. Authors: Rajesh Pasupuleti; Ravi Vadapalli; Christopher Mader
6. AI-assisted Cyber Security Exercise Content Generation: Modelling a Cyber Conflict. Authors: Alexandros Zacharis; Razvan Gavrila; Constantinos Patsakis; Demosthenes Ikonomou.
7. Al-Khshali, H. H., & Ilyas, M. (2023). Impact of portable executable Header features on malware detection accuracy. *Computers, Materials & Continua, 74*(1), 153–178.

8. Alalwan, J. A. A. (2022). Roles and challenges of AI-based cybersecurity: A Case study. *Jordan Journal of Business Administration, 18*(3), 437–456.
9. Arasada, S. (2021). These four challenges in adopting machine learning can lower your ROI and sabotage success. Forbes.
10. Ariffin, N. H. M., & Maskat, R. (2021). A proposal of ethical competence model for cyber security organization. *Indonesian Journal of Electrical Engineering and Computer Science, 24*(3), 1711–1717.
11. Brison, R., Wimmer, H., & Rebman, C. M. (2022). Botnet intrusion detection: A modern architecture to defend a virtual private cloud. *Issues in Information Systems, 23*(3), 114–127.
12. Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in CyberSecurity: A survey. *IEEE Access, 10*, 93575–93600.