Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 3 Issue 2 (2023)

Use Of Enhanced Artificial Intelligence in Security Business Management in The Digital Economy Era

Dr. Sarika
Assistant Professor, Management, Gitarattan International Business School, GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY, DELHI
dr.sarikatanwar2427@gmail.com

Dr. Mohd Naved
Associate Professor (Analytics), SOIL School of Business Design, Manesar, Haryana, India
mohdnaved@gmail.com
https://orcid.org/0000-0003-3357-9947

Dr. Amit Jain
Professor, Computer science and engineering department, O P Jindal University, Raigarh
amitscjain@gmail.com

Dr. Niharika Bajeja
Associate Professor, Economics and Marketing, Faculty of Management Studies, Marwadi University, Rajkot, Gujarat, India

Pranjal Rawat
Research Scholar, School of Management, Graphic Era Hill University, Dehradun, Uttrakhand
rawatpranjal89@gmail.com

Dr. Christabell Joseph
Associate Professor, School of Law, Christ University
christabell.joseph@christuniversity.in

Abstract

Enhanced use of artificial intelligence (AI) in security business management offers the potential to reduce costs, increase efficiency, and improve danger detection in the age of the digital economy. Examples from businesses like Amazon, Cisco Systems, and JP Morgan Chase highlight how AI is revolutionizing security procedures. Nonetheless, there are obstacles because of privacy and ethical issues as well as an ongoing skills shortage in the field. The U.S. lacks 150,000 AI specialists, which is preventing AI from reaching its full potential, according to the 2020 LinkedIn AI report. This comprehensive analysis delves into the complex world of artificial intelligence (AI) in security, providing advice for enterprises and highlighting the critical need to close the skills gap in order to effectively utilize AI's potential for safeguarding operations in the age of the digital economy.

Keywords: Artificial Intelligence (AI), Digital, security, economy, technology, Cybersecurity.

Introduction

The main aim of the project is to discuss the use of enhanced artificial intelligence in security business management in the digital economy era. Businesses may now operate more quickly than ever thanks to the advancement of information technology, especially when it comes to providing customer services. These cutting-edge operational solutions have made it feasible for them to manage their resources effectively and appropriately as well. However, most organisations still do not completely understand the benefits that adopting artificial intelligence and related technology could bring about. Many corporations and governments are currently looking into these facets of knowledge management to make the most of these new forms of computing power that are emerging in our digital age. Executives in business must therefore devise strategies that will enable them to gain from the advantages that so-called artificial intelligence is

bringing about. Artificial intelligence can be used by businesses to cut costs and improve operational efficiency (Bharadiya, 2023). There are many areas of interest and economic prospects as a result of the current situation. They become a hub for discovery thanks to cloud AI, which also makes the clouds accessible for reporting and modifying technical data. In completely AI-driven packages, businesses can modify raw memory structures or databases as significant facts (Wang et al., 2020).

Problem Statement

The insufficient use of enhanced artificial intelligence in safety company management in the context of the digital economy era is the problem statement for this research. Even with all of AI technology's recent advances, a lot of companies and organizations still don't realize all of its potential advantages. The problem is that AI-driven solutions are not well integrated, especially when it comes to security and data management. This makes it difficult to save costs, increase operational efficiency, and extract useful insights (Kinelski, 2020). In order to assist organizations, achieve the promise of AI in optimizing operations and strengthening security measures, this research intends to solve this issue by exploring the opportunities and limitations in applying AI for safety business management.

- The aim of this study is to optimize the advantages of improved artificial intelligence for security company management in the context of the digital economy.
- This study aims to achieve three distinct goals. Initially, to look into the obstacles and difficulties that now stand in the way of the successful incorporation of improved machine learning into security company leadership procedures.
- The second objective is to recognize and evaluate the economic benefits and prospects that artificial intelligence (AI) technology presents for improving operational efficiency, cutting costs, and bolstering security measures.
- Thirdly, to provide plans and suggestions for companies to fully utilize AI technologies, with the ultimate goal of fostering the development of a safer and more effective digital economy ecosystem.

Research background

Businesses have attempted to take advantage of opportunities by integrating the most recent developments in intelligent manufacturing into the manufacturing industry. The switch to smart production from conventional manufacturing in the previous two years is a great illustration of such a circumstance. Smart production, on the other hand, focuses on utilising and integrating intelligent machinery in production contexts (Wang et al., 2022). In addition to buying behaviour, using a card in another nation shortly after using it elsewhere or attempting to withdraw can be prevented by buying and selling special devices. A further advantage of AIfraud detection is that the system is confident in its dominance. These integrated devices connect to sensors and other components, and such systems can automatically gather pertinent data sets in real-time to support planning and decision-making. Even if a business owner does not recognise a difference between the company's existing assets and those being used by future generations, the implications of adopting AIare huge, as shown by the tools that flow from it. AI is now being used by almost all contemporary businesses to lower production costs and save time. By investing in artificial intelligence programmes, many hanks place a priority on strategic technology development in order to better serve their clients, boost efficiency, and boost sales. The global era has changed over time; media outlets have switched from television, radio, and newspapers to the Internet and are gradually embracing artificial intelligence (Jain, & Pandey, 2019). AI can speed up fact-processing, evaluate consumer dangers, and decide how customers will be controlled going forward. The fact that a significant portion of their historical data is still kept in paper files and not digital spaces is one of the most difficult situations that large organisations, banks, insurance companies, and financial institutions confront when deploying AI Before employing consultants to create AI solutions or purchasing AI software, financial institutions should make sure they digitise historical records. A quirk learning machine must be educated in virtual reality. Any stage of the business process, including the front, middle, and back offices, may apply artificial intelligence (Mosteanu, 2020). In any industry, artificial intelligence can be employed.

Literature Review

Role of AI in Business Management

With the use of AI technology, machines can perform complicated tasks including watching, learning, planning, and making judgements in order to solve problems. Predictive analytics, process automation, customer analytics, security monitoring, and job optimisation are some of the main applications of artificial intelligence in business management. Based on their present business data, businesses can use predictive analytics to forecast future trends. Jones (2022) argues, artificial intelligence has advanced from being a trendy term to being used in driverless cars and winning games that cannot be won. In today's technological environment, managers have a wide range of tools at their disposal to boost team productivity and ensure a steady flow of clients or leads for their company. They can free themselves from boring activities and bring more value to the company with the aid of AI. Let's look at how managers can use artificial intelligence in corporate management to make better judgements.

Consider the case of investment managers. Due to the rise of robot-advisors replacing human fund managers, money management is predicted to experience job losses of over 40% in the financial sector (CNBC, 2022). There is a bright side to what might initially appear to be a negative. This is a chance to sharpen one's abilities and take advantage of the greater accessibility of high-quality, quick data, especially if one is already investing a lot of time in data collection, analysis, organisation, and presentation in order to spot prospective issues, difficulties, and advancement.

AI and Cybersecurity

According to Hoffman (2021), artificial intelligence is even a crucial ally when trying to find weaknesses in computer network defences. Unbelievably, by observing patterns in data input, AI systems may detect cyberattacks and other cyberthreats. When a danger is identified, it can go back through the data to locate the source and aid in preventing further threats. The additional set of eyes will be very helpful in maintaining the infrastructure because they are as vigilant and constant as AI. As per Shamiullah (2019), the application of AI in cyber security has grown in importance as the number of cyberattacks has increased. AI can deliver quicker and more precise answers for anything from threat identification to incident response, increasing the overall efficacy of cyber security measures.

- The correct AI cybersecurity solutions can not only identify recent dangers within a network of an organisation, but they can also find unidentified hazards. Such unidentified threats have the potential to seriously harm the network. To stop such assaults, it is now crucial to deploy contemporary network security technologies like AI. With the correct cyber security council, AI and business can lessen the effects of hacking or the millions of attacks carried out by hackers with various goals (Mosteanu, 2022).

- Vulnerability management is essential to protecting a network within a company. Vulnerability management can be achieved by analysing and accessing the current security measures and combining AI with cyber security. In essence, it aids in system assessment quicker than cybersecurity personnel, which increases the capacity for critical thought. In general, concentrating on According to Dasgupta et al. (2023), AI for cybersecurity has enabled firms to control vulnerability and safeguard corporate systems in a timely manner.

- The initial step in securing a company's network is threat detection. Businesses would be shielded from any network damage that could not be repaired if they could immediately identify some untrustworthy data.AI is a useful tool for network security because it searches the entire network and identifies potential dangers before they can do any harm. Unlike a person, AI completes such jobs more quickly and makes security tasks simpler.

- As hackers employ new strategies every day, the challenges that businesses confront are ever-evolving. It becomes difficult for a corporation to prioritise security tasks as a result. Furthermore, carelessness and human error are two of the major risks that complicate security (Jain, &Pandey,2019). This is where AI cybersecurity solutions may identify various assaults, assist businesses in prioritising them, and prevent them as necessary.

- There are numerous tasks that even a small organisation must complete on a company's network. It implies that a significant amount of data is moved daily between customers and enterprises. They require data protection from hostile assaults because of this, yet cybersecurity cannot find every threat. But with AI cybersecurity solutions, any

threat disguising itself as routine activity can be easily detected. It can quickly scan through huge amounts of traffic and data because of its automotive nature. In the modern world, it might be difficult to keep the network and data secure. But according to Dhoni & Kumar (2023), by using AI to bolster their security architecture, businesses may make a significant step towards becoming safer.

Use if AI in digitally economic era

Despite the fact that academics categorise AI in many ways, they agree that AI refers to machines that are not restricted by the rigidity and constraints of human cognition. As a result, AI can be taught to use massive, complicated datasets to produce decisions that are effective, accurate, and consistent. Such abilities are crucial for businesses to develop competitive advantages in the digital economy. According to Pei et al. (2020), for instance, a crucial competitive advantage in the current market is a personalised client experience. As a result, businesses must employ AI to compile high-quality customer experience data in order to provide personalised service. Gaining a competitive edge can result in more revenues and/or lower costs. According to Fotheringham & Wile (2022), the use of AI customer support chatbots results in a 0.22% anomalous stock return, with B2B companies benefiting more than their B2C counterparts. In fact, studies have shown time and time again that the stock market reacts favourably to companies adopting AI. AI systems boost revenue through boosting worker output, boosting consumer responsiveness, establishing competitive pricing, and developing exclusive resources. The main problem for these businesses is that they cannot electronically or virtually stock merchandise, unlike Amazon, Airbnb, or Apple, thus they must find another way to acquire a competitive advantage. The narrative of the tortoise and the hare, in which the hare eats the tortoise for lunch, is more representative of the future of rivalry than the David and Goliath battle (Jain et al., 2019). The future's buzzwords are nimbleness, adaptability, resilience, and agility, which offer a more competitive advantage than traditional scale and size. Supply chain businesses are aware of this problem, but many have invested millions or even billions of dollars in manufacturing, transportation, and other infrastructure, and they are unable to start over from scratch. To achieve the highest level of agility, they should instead use and change their current investments. In other words, they must change engines mid-air while in full flight. AI is useful in this situation. 90 to 95 percent of supply chain companies are now working on AI/ML pilot projects, but many of them are just interested in the newest technology and not where it may have the biggest impact (EPS News, 2020). When AI can comprehend what is happening in the supply chain, make sense of it, learn from it, and then provide people with the necessary decision assistance, it is most effective. When it comes to supply chain transformation, AI may actually make a difference through this so-called augmented supply chain transformation. While automating decisions may be feasible in some circumstances and might make sense, the effect threshold for those decisions is minimal (Panwar et al., 2021). Human responsibility and judgement must always be a component of the decision-making process for those decisions that truly affect supply chain change. Manual labour is present everywhere. One can save money if they can automate such manual procedures.

Because artificial intelligence (AI) has the ability to change existing business practices and protect against emerging cyber dangers, it has garnered significant attention when it comes to using AI for security business management in the digital economy (Zhou, 2022). This review of the literature will examine important facets of the use of AI in security management, emphasizing noteworthy cases and pertinent information.

AI Applications in Security Business Management

There are several uses for artificial intelligence in security company leadership. For example, businesses such as Amazon have successfully used AI-powered security systems to safeguard their warehouses. Computer vision is used by Amazon's AWS DeepLens to keep an eye on worker safety and the security of products. These systems have the ability to stop security breaches, guarantee compliance, and identify irregularities.

Palantir Technologies, which serves clients in a variety of industries, including defence and security, and offers software powered by AI for integrating information and analysis, is another noteworthy example (Limna *et al.* 2022). Their platform, Gotham, helps businesses keep ahead of possible security threats by supporting predictive modelling and threat analysis.

Cost Reduction and Efficiency

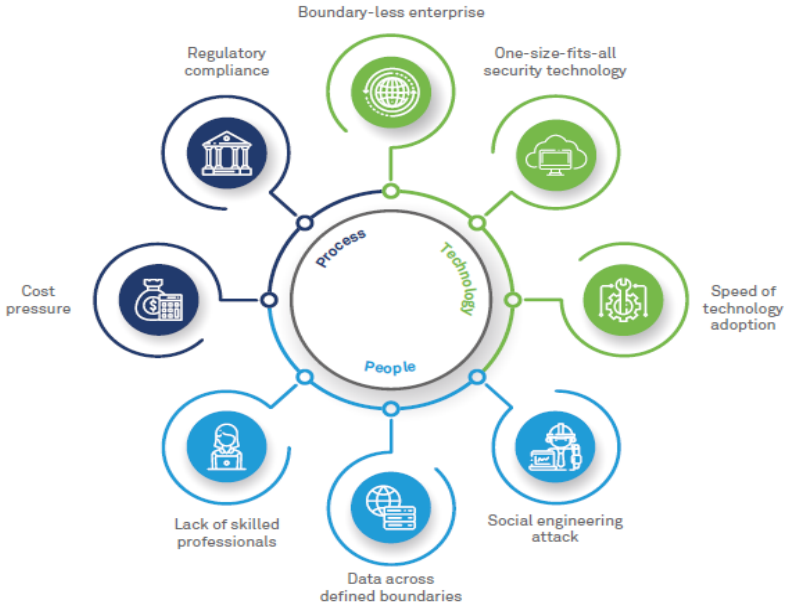
Cost savings is one of the main benefits of implementing AI in security business management. According to PwC's 2020 Global Trust in Digital Insights Survey, businesses that completely integrate AI into their cybersecurity policies see a 53% decrease in total security incidents and related expenses. Task automation, faster event detection, and more effective response times are the causes of this decrease.

Enhanced Threat Detection and Prevention

AI can greatly improve threat identification and mitigation. In order to detect and neutralize cyber-attacks, Cisco's Talos Data Group analyses vast amounts of data using AI and machine learning. This strategy improves their capacity to proactively reduce possible security threats (Agrawal *et al.* 2022). In order to help stop illegal transactions, JP Morgan Chase has implemented AI algorithms in the banking sector to evaluate and identify fraudulent activity in real-time.

Figure: 1

Future of Cyber security



(Source: wipro.com, 2023)

Real-time Monitoring and Response

A crucial component of AI in security is real-time monitoring. Machine learning is used by Darktrace, a powered by AI cybersecurity startup, to recognize and address risks as they arise. In the contemporary technological era, where risks are evolving quickly and necessitating quick action, this expertise is vital.

Challenges and Barriers

The use of AI in security company management is not without its difficulties, despite its possible advantages. Concerns about data privacy and ethics provide a big obstacle. Sensitive data must be handled and stored by businesses appropriately. If you don't, there could be serious legal and reputational repercussions (Alrfai *et al.* 2023). For example, Facebook came under regulatory and public criticism for data privacy issues, highlighting the significance of treating data ethically.

Furthermore, the skills gap continues to be a major obstacle. Businesses require professionals to handle and deploy AI technologies efficiently. The complete integration of AI in security oversight may be hampered by the lack of skilled AI

experts. 2020 LinkedIn research stated that there was a deficiency of over 150,000 AI specialists in the United States alone.

Figure: 2

Influence of AI to your security operations

(Source: it-explained.com, 2023)

Methodology

This study's technique, which is based on interpretivism and logical reasoning, takes a secondary approach. Secondary research entails the examination of previously published works, studies, and pertinent data sources in order to generate new ideas and provide a thorough grasp of the topic. Interpretivism is in line with this research because it enables the analysis of intricate ideas—like the incorporation of AI in security company management—in the framework of various viewpoints and practical implementations. The study will employ a deductive approach, starting with well-established ideas and previous research to generate hypotheses and a framework. In order to better understand the adoption of AI in security business administration in the context of the digital economy, the study will first compile and evaluate the body of prior scholarly articles, reports, research papers, and industry data (Mohammed, 2021). The next step will be data analysis and synthesis to find patterns and make connections. This method seeks to give a thorough overview of the application of improved intelligent technology in security company administration through an organized and empirically supported investigation of the topic.

Analysis

In the age of the digital economy, the incorporation of increased artificial intelligence (AI) in the security management of companies has become a revolutionary force that presents enterprises with both benefits and challenges (Bharadiya, 2023). It will explore important facets of AI use in security in this in-depth research, using statistics, industry trends, and real-world examples to give readers a thorough grasp of this ever-changing environment.

Cost Reduction and Efficiency Gains

Security systems powered by AI have demonstrated amazing promise in cutting costs and increasing operational effectiveness. According to data from a 2020 PwC Global Trust in Digital Insights Survey, companies who fully integrated AI into their cybersecurity plans saw a 53% decrease in total security incidents and related expenses. This is mostly because regular tasks have been automated, and AI is better than manual techniques in detecting and responding to dangers (Zhang, Ma & Cui, 2021). For example, AWS DeepLens from Amazon uses AI and computer vision to improve security and safety in its warehouses. It streamlines processes and protects against theft with continuous tracking and anomaly detection.

Enhanced Threat Detection and Prevention

Businesses such as Cisco, which uses artificial intelligence and machine learning in its Talos Intel Group, are prime examples of how AI can improve threat detection and prevention. Cisco's AI systems can detect and neutralize cyber

threats instantly by evaluating enormous volumes of data, offering an anticipatory approach to cybersecurity. AI in safety is also not just used in digital environments (Ahmed *et al.* 2021). The benefits extend to physical security as well. AI-driven facial recognition systems, such as those employed by law enforcement or at airports, can quickly detect possible threats, improving public safety.

Real-time Monitoring and Response

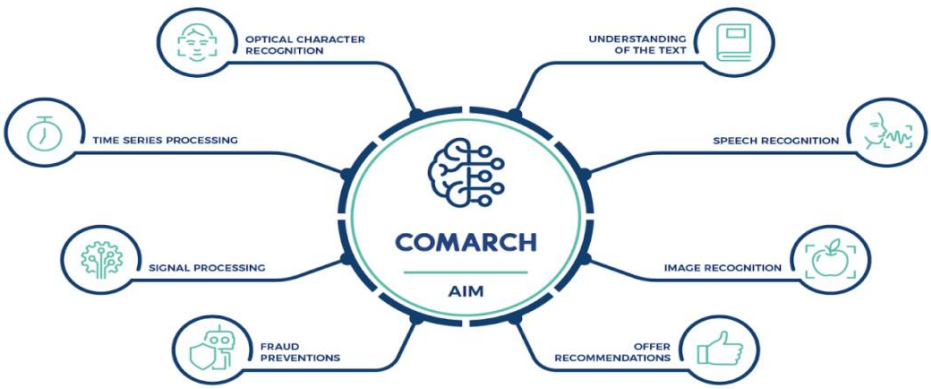
Monitoring in real time is essential in the ever-changing digital world. One such example is the cybersecurity firm Darktrace, which uses AI. Their machine learning systems are able to identify anomalies, analyse network data continually, and react to threats instantly. This feature guarantees that security vulnerabilities are dealt with quickly, minimizing possible harm. In sectors such as finance, real-time tracking is essential (Spence, 2021). In order to stop illegal transactions and safeguard customer assets, JP Morgan Chase employs artificial intelligence (AI) to track and identify fraudulent activity.

Data Privacy and Ethical Concerns

Important questions are also brought up by the use of AI in security, mainly in relation to ethics and data protection. The Cambridge Analytica controversy, in which private information was exploited for political ends, emphasizes how crucial it is to handle data responsibly. Businesses have to walk a tightrope between utilizing AI for safety and protecting people's privacy. The European Data Protection Regulation (GDPR) places strict limitations on the gathering and use of data. Fines for noncompliance may be rather high (Handayani & Agustina, 2022). As a result, businesses have made significant investments in AI-driven data compliance solutions to make sure they both meet legal requirements and uphold strong security.

Figure: 3

Artificial Intelligence Management



(Source: comarch.com, 2023)

The Skills Gap

The persisting skills gap in the sector is impeding the enormous potential of AI in security leadership. This worry was emphasized by the 2020 LinkedIn AI research, which showed that there is an alarming scarcity of almost 150,000 AI specialists in the US. The lack of qualified workers is a major obstacle to the efficient application of AI in security procedures. These professionals are needed by businesses to develop, deploy, and oversee artificial intelligence (AI) systems that can defend sensitive data and fend off changing threats. Organizations struggle with underutilizing AI's transformational potential when they lack a skilled workforce. In order to fully realize AI's promise to improve security management, it is essential to address this crucial skills gap because it has a direct influence on the capacity to keep ahead of constantly changing operational difficulties and cyber threats.

Recommendations for Businesses

Given the benefits and difficulties that artificial intelligence (AI) presents for security business management, the following suggestions can help enterprises successfully navigate this terrain:

A. Invest in Worker Training:	To close the skills gap, businesses should spend in educating and enhancing the abilities of their employees. A pool of competent professionals capable of handling AI systems and data ethically can be produced by offering educational and professional development opportunities.
B. Give Privacy of Data and Ethics First Priority:	When adopting AI, privacy concerns and ethical considerations need to be the top priorities. To preserve public trust and safeguard individual privacy, businesses must implement stringent data processing policies and adhere to all applicable rules.
C. Preserve Flexibility and Agility:	Organizations want flexible AI systems that can adjust to novel security threats in a constantly shifting threat landscape. Robust security requires flexibility in the construction of systems as well as the capacity to learn and adapt on a constant basis.
D. Work Together and Exchange Insights:	Industry collaboration is essential (Grover, Kar, Dwivedi, 2022). Exchange of best practices and insights can assist firms in staying ahead of new risks. In this context, industry-specific forums and partnerships can be helpful.

Industry-Specific Examples

Various sectors have developed AI security management applications. One such example is the finance industry. AI algorithms are used by JP Morgan Chase to identify and stop fraudulent activity. The financial system's integrity has been preserved and client protection has been aided by its real-time tracking and reaction capabilities.Another area where AI has significantly improved security is the healthcare sector. Medical devices are shielded from cyberattacks by AI-driven systems, such as those offered by MedCrypt. These systems guarantee the security and safety of vital medical devices, like infusion pumps and pacemakers. AI is used in retail to secure real stores as well as online. Walmart uses artificial intelligence (AI) and computer vision to monitor stores and identify any theft or breaches of security. This helps clients have a better shopping experience while also protecting inventories.In the age of the digital economy, there is tremendous potential for cost savings, increased productivity, improved detection of threats, and real-time monitoring through the integration of improved AI into safety business management. Businesses such as JP Morgan Chase, Amazon, and Cisco provide as examples of how AI is being used in security (Spence, 2021). Nonetheless, there are difficulties because of the skills gap as well as ethical and data privacy issues. Businesses are able to take full advantage of AI's potential to protect their businesses in the digital age by solving these concerns and following best practices.

Conclusion

In conclusion, the application of artificial intelligence to cybersecurity is poised to further revolutionise the field by enhancing threat detection and response methodologies. Although employing Al in cybersecurity may have biases and difficulties, its capacity to change and adapt to new cyberthreats makes it an essential component in preventing cyberattacks in the digital age. Despite growing interest in AI and the digital economy, there remain certain obstacles to the use of AI in this sector. For instance, how to leverage cutting-edge AI technology to intellectualise economic processes, how to formalise the relationship between the digital economy and AI, and how to train an effective big AI model with comparatively low computational resource consumption. As a result, there is a great chance to research trustworthy, dependable, and effective AI technologies that are focused on the digital economy.

Artificial intelligence, which activates corporate processes, boosts productivity, and provides a variety of ways to speed up verbal interchange techniques, is currently present in practically every company organisation. Many jobs that used to

be done by staff members and employees are now carried out by AI software and automation by AI systems. The change to an automated operating environment has caused businesses to lose a lot of money, save a lot of time, and regain profits slowly. This article describes the role of AI, tool adoption, and cloud computing in the enterprise. AI-assisted automation for various ways of working has advanced many businesses and organisations' production and control.

Future Scope and Limitations

Promising prospects are ahead for AI in security company management. Threat identification, reaction, and prediction are predicted to undergo a radical transformation with the introduction of quantum computing and improved machine learning algorithms, among other AI technological developments. AI-driven security solutions will become more widespread as cloud computing and the Internet of Things (IoT) evolve, providing real-time monitoring and protection for a variety of businesses (Bharadiya, 2023). AI adoption in safety management is constrained by challenges including privacy concerns, ethical concerns, and the requirement for ongoing skill improvement, despite its potential. Concerns about bias in AI systems as well as regulatory issues must be addressed. Furthermore, obstacles to wider adoption include the high cost of installation and the dynamic nature of cyber threats.

References

1. Jain, A. K. Pandey, (2019), "Modeling And Optimizing Of Different Quality Characteristics In Electrical Discharge Drilling Of Titanium Alloy (Grade-5) Sheet" Material Today Proceedings, 18, 182-19, https://doi.org/10.1016/j.matpr.2019.06.292
2. Jain, A. K. Pandey, (2019), "Modeling And Optimizing Of Different Quality Characteristics In Electrical Discharge Drilling Of Titanium Alloy (Grade-5) Sheet" Material Today Proceedings, 18, 182-191, https://doi.org/10.1016/j.matpr.2019.06.292
3. Jain, A.K.Yadav & Y. Shrivastava (2019), "Modelling and Optimization of Different Quality Characteristics In Electric Discharge Drilling of Titanium Alloy Sheet" Material Today Proceedings, 21, 1680-1684, https://doi.org/10.1016/j.matpr.2019.12.010
4. Agrawal, R., Wankhede, V. A., Kumar, A., Upadhyay, A., & Garza-Reyes, J. A. (2022). Nexus of circular economy and sustainable business performance in the era of digitalization. *International Journal of Productivity and Performance Management*, *71*(3), 748-774. https://repository.londonmet.ac.uk/6391/1/Revised-Manuscript.pdf
5. Ahmed, S., Hossain, M. F., Kaiser, M. S., Noor, M. B. T., Mahmud, M., & Chakraborty, C. (2021). Artificial intelligence and machine learning for ensuring security in smart cities. In *Data-Driven Mining, Learning and Analytics for Secured Smart Cities: Trends and Advances* (pp. 23-47). Cham: Springer International Publishing. https://www.researchgate.net/profile/Md-Hossain-823/publication/351168298_Artificial_Intelligence_and_Machine_Learning_for_Ensuring_Security_in_Smart_Cities/links/6101862a0c2bfa282a09f8b0/Artificial-Intelligence-and-Machine-Learning-for-Ensuring-Security-in-Smart-Cities.pdf
6. Alrfai, M. M., Alqudah, H., Lutfi, A., Al-Kofahi, M., Alrawad, M., & Almaiah, M. A. (2023). The influence of artificial intelligence on the AISs efficiency: Moderating effect of the cyber security. *Cogent Social Sciences*, *9*(2), 2243719. https://www.tandfonline.com/doi/pdf/10.1080/23311886.2023.2243719
7. Bharadiya, J. P. (2023). A Comparative Study of Business Intelligence and Artificial Intelligence with Big Data Analytics. *American Journal of Artificial Intelligence*, *7*(1), 24. https://www.researchgate.net/profile/Jasmin-Bharadiya-4/publication/371988416_A_Comparative_Study_of_Business_Intelligence_and_Artificial_Intelligence_with_Big_Data_Analytics/links/64b58091b9ed6874a52688d7/A-Comparative-Study-of-Business-Intelligence-and-Artificial-Intelligence-with-Big-Data-Analytics.pdf
8. Bharadiya, J. P. (2023). Machine Learning and AI in Business Intelligence: Trends and Opportunities. International Journal of Computer (IJC), 48(1), 123-134. https://www.researchgate.net/profile/Jasmin-Bharadiya-4/publication/371902170_Machine_Learning_and_AI_in_Business_Intelligence_Trends_and_Opportunities/links/649afb478de7ed28ba5c99bb/Machine-Learning-and-AI-in-Business-Intelligence-Trends-and-Opportunities.pdf?origin=journalDetail&_tp=eyJwYWdlIjoiam91cm5hbERldGFpbCJ9

9. Cognitiveautomation.com (2020), "Can Artificial Intelligence Really Help the Digital Economy?" 2020, www.cognitiveautomation.com/resources/can-artificial-intelligence-really-help-the-digital-economy.
10. comarch.com, 2023, Artificial Intelligence Management, Available at: https://www.comarch.com/artificial-intelligence-management/ [Accessed on: 13/10/2023]
11. Dasgupta, S., Yelikar, B. V., Naredla, S., Ibrahim, R. K., & Alazzam, M. B. (2023, May). AI-Powered Cybersecurity: Identifying Threats in Digital Banking. In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 2614-2619). IEEE. https://www.researchgate.net/profile/Malik-Alazzam-2/publication/372616203_Leveraging_Big_Data_in_Financial_Institutions_and_Law_Enforcement_Challenges_and_Opportunities/links/64ec81dd40289f7a0fbeb6ce/Leveraging-Big-Data-in-Financial-Institutions-and-Law-Enforcement-Challenges-and-Opportunities.pdf
12. Dhoni, P., & Kumar, R. (2023). Synergizing Generative AI and Cybersecurity: Roles of Generative AI Entities, Companies, Agencies, and Government in Enhancing Cybersecurity. https://www.techrxiv.org/articles/preprint/Synergizing_Generative_AI_and_Cybersecurity_Roles_of_Generative_AI_Entities_Companies_Agencies_and_Government_in_Enhancing_Cybersecurity/23968809/1/files/42024516.pdf
13. Grover, P., Kar, A. K., & Dwivedi, Y. K. (2022). Understanding artificial intelligence adoption in operations management: insights from the review of academic literature and social media discussions. *Annals of Operations Research*, *308*(1-2), 177-213. https://e-tarjome.com/storage/panel/fileuploads/2022-05-28/1653730839_e16525.pdf
14. Handayani, I., & Agustina, R. (2022). Starting a digital business: Being a millennial entrepreneur innovating. *Startupreneur Business Digital (SABDA Journal)*, *1*(2), 126-133. https://journal.pandawan.id/sabda/article/download/113/112
15. Hang, Haiming, and Zhifeng Chen. "How to Realize the Full Potentials of Artificial Intelligence (AI) in the Digital Economy? A Literature Review." Journal of Digital Economy, vol. 1, no. 3, Dec. 2022, https://doi.org/10.1016/j.jdec.2022.11.003.
16. Hoffman, W. (2021). AI and the Future of Cyber Competition. CSET Issue Brief, 1-35. https://pdfs.semanticscholar.org/8e7b/feb766d13a0a311bff7ae3b83e7593d08ff0.pdf
17. http://www.parkjonghyuk.net/lecture/2023-1st-lecture/cps/jbh1.pdf
18. Iacurci, Greg. "Robo-Advisors Are Growing in Popularity. Can They Really Replace a Human Financial Advisor?" CNBC, 16 Jan. 2022, www.cnbc.com/2022/01/16/robo-advisors-are-gaining-popularity-can-they-replace-a-human-advisor.html. Accessed 2022. https://www.cnbc.com/2022/01/16/robo-advisors-are-gaining-popularity-can-they-replace-a-human-advisor.html
19. it-explained.com, 2023, Influence of AI to your security operations Available at: https://it-explained.com/words/ai-driven-security-operations-explained-explained [Accessed on: 13/10/2023]
20. Jones, L. (2022). The future of warfare is irregular. Fletcher F. World Aff., 46, 107. http://www.fletcherforum.org/s/Jones-2a_APPROVED.pdf
21. Kinelski, G. (2020). The main factors of successful project management in the aspect of energy enterprises' efficiency in the digital economy environment. *Polityka Energetyczna–Energy Policy Journal*, *23*(3), 5-20. https://epj.min-pan.krakow.pl/pdf-126435-55454?filename=Themainfactorsof.pdf
22. Limna, P., Jakwatanatham, S., Siripipattanakul, S., Kaewpuang, P., & Sriboonruang, P. (2022). A review of artificial intelligence (AI) in education during the digital era. *Advance Knowledge for Executives*, *1*(1), 1-9. https://www.researchgate.net/profile/Pongsakorn-Limna/publication/361926050_A_Review_of_Artificial_Intelligence_AI_in_Education_during_the_Digital_Era/links/62cd55ebcab7ba7426e90dad/A-Review-of-Artificial-Intelligence-AI-in-Education-during-the-Digital-Era.pdf
23. Mohammed, I. A. (2021). The interaction between artificial intelligence and identity and access management: an empirical study. *International Journal of Creative Research Thoughts (IJCRT), ISSN*, *2320*(2882), 668-671. https://www.researchgate.net/profile/Ishaq-Azhar-Mohammed/publication/353888035_The_Interaction_Between_Artificial_Intelligence_and_Identity_Access_M

anagement_An_Empirical_study/links/6116a4731ca20f6f861e49df/The-Interaction-Between-Artificial-Intelligence-and-Identity-Access-Management-An-Empirical-study.pdf

24. Mosteanu, N. R. (2020). ARTIFICIAL INTELLIGENCE AND CYBER SECURITY â€“FACE TO FACE WITH CYBER ATTACK â€“A MALTESE CASE OF RISK MANAGEMENT APPROACH. Ecoforum Journal, 9(2). http://www.ecoforumjournal.ro/index.php/eco/article/download/1059/672
25. Mosteanu, N. R. (2020). ARTIFICIAL INTELLIGENCE AND CYBER SECURITY â€“FACE TO FACE WITH CYBER ATTACK â€“A MALTESE CASE OF RISK MANAGEMENT APPROACH. Ecoforum Journal, 9(2). http://www.ecoforumjournal.ro/index.php/eco/article/download/1059/672
26. Pei, X. L., Guo, J. N., Wu, T. J., Zhou, W. X., & Yeh, S. P. (2020). Does the effect of customer experience on customer satisfaction create a sustainable competitive advantage? A comparative study of different shopping situations. Sustainability, 12(18), 7436. https://www.mdpi.com/2071-1050/12/18/7436/pdf
27. Shamiulla, A. M. (2019). Role of artificial intelligence in cyber security. International Journal of Innovative Technology and Exploring Engineering, 9(1), 4628-4630. https://www.academia.edu/download/85177722/A6115119119.pdf
28. Spence, M. (2021). Government and economics in the digital economy. *Journal of Government and Economics*, *3*, 100020. https://www.sciencedirect.com/science/article/pii/S2667319321000203
29. V. Panwar, D.K. Sharma, K.V.P. Kumar, A. Jain & C. Thakar, (2021), "Experimental Investigations And Optimization Of Surface Roughness In Turning Of EN 36 Alloy Steel Using Response Surface Methodology And Genetic Algorithm" Materials Today: Proceedings, https://Doi.Org/10.1016/J.Matpr.2021.03.642
30. Wan, J., Li, X., Dai, H. N., Kusiak, A., Martinez-Garcia, M., & Li, D. (2020). Artificial-intelligence-driven customized manufacturing factory: key technologies, applications, and challenges. Proceedings of the IEEE, 109(4), 377-398. https://arxiv.org/pdf/2108.03383
31. Wang, B., Zheng, P., Yin, Y., Shih, A., & Wang, L. (2022). Toward human-centric smart manufacturing: A human-cyber-physical systems (HCPS) perspective. Journal of Manufacturing Systems, 63, 471-490.
32. wipro.com , 2023, Eliminating the complexity in cybersecurity with Artificial Intelligence Available at: https://www.wipro.com/cybersecurity/eliminating-the-complexity-in-cybersecurity-with-artificial-intelligence/ [Accessed on: 13/10/2023]
33. Zhang, S., Ma, X., & Cui, Q. (2021). Assessing the impact of the digital economy on green total factor energy efficiency in the post-COVID-19 era. *Frontiers in Energy Research*, *9*, 798922. https://www.frontiersin.org/articles/10.3389/fenrg.2021.798922/full
34. Zhou, Y. (2022). The application trend of digital finance and technological innovation in the development of green economy. *Journal of Environmental and Public Health*, *2022*. https://www.hindawi.com/journals/jeph/2022/1064558/