WEP
Warwick
Evans
Publishing

Transactions on Economics, Business and Management Research
ISSN: 2960-1789, eISSN: 2960-2254 | Volume 14
AFTEM 2024

Analysis of Problems and Countermeasures of Artificial Intelligence in Business Analytics

Weiye Chen*

The Affiliated Foreign Language School of SCNU, Guangzhou 510000, China

*Corresponding Author: 25weiye.chen@highschool.scnufl.com

Abstract. The use of Artificial Intelligence (AI) in business analytics presents significant opportunities and challenges. This study analyzes the major issues in AI implementation, such as data accuracy, high initial cost, and privacy protection. To address these issues, the study proposes countermeasures, including strengthening data governance, reducing initial costs through cloud-based AI services, and enhancing data privacy protection measures. The results of the study point out the specific manifestations and solutions to these problems and provide actionable strategic recommendations for enterprises in AI applications. This study has significant application value for how enterprises can improve decision-making efficiency, reduce operational risks, and achieve sustainable development through AI.

Keywords: Business analytics; artificial intelligence; data governance; privacy protection; initial cost reduction.

1. Introduction

All manuscripts Must be in English, also the table and figure texts, otherwise, we cannot publish your paper.

Please keep the second copy of your manuscript in your office. When receiving the paper, we assume that the corresponding authors grant us the copyright to use the paper for the book or journal in question. Should authors use tables or figures from other Publications, they must ask the corresponding publishers to grant them the right to publish this material in their paper.

Use italic for emphasizing a word or phrase. Do not use boldface typing or capital letters except for section headings (cf. remarks on section headings, below).

2. Introduction

The application of Artificial Intelligence in business analytics is of immense significance, providing enterprises with fast and accurate decision support, reducing operational costs, and improving the efficiency of resource allocation. In the modern market environment, business analytics provides important support for the quality of response and resource utilization of enterprises. The application of AI technology not only improves the number of tasks in business analytics, but also leads to a significant improvement in business accuracy and analysis efficiency [1].

In recent years, with the rapid development of AI in computational power, data analysis and deep learning, its application in business analytics has become more and more popular and demonstrated significant application value.AI technology plays an important role in the operation management and market prediction of enterprises, helping them to improve their competitiveness and market flexibility. However, the wide application of AI also faces many challenges, such as data accuracy, initial cost and privacy protection [2].

Although AI has made important achievements in business analytics, there are still some problems that need to be solved. Therefore, this study provides an in-depth analysis of these problems and proposes potential countermeasures to solve them. These countermeasures can not only help enterprises better cope with the challenges in AI application, but also help them achieve more efficient

and sustainable development. By strengthening data governance, reducing the cost of AI technology implementation, and implementing strict data privacy protection measures, enterprises can effectively enhance their market competitiveness and lay a solid foundation for future business development.

3. Issues with AI in Business Analytics

3.1. Data accuracy and dependency

AI systems are highly dependent on large amounts of data for prediction and optimization in business analytics. However, if the data source is inaccurate or incomplete, the AI's decision-making will be biased with it, which will affect the analysis of the data and even have an impact on the original database and memory. For example, Uber's dynamic pricing mechanism relies on AI's real-time analysis of market supply and demand, but during the outbreak, the market data changed drastically, and the AI system failed to fully grasp this change, leading to statistical confusion and dramatic pricing fluctuations, and this not only affected consumer and driver satisfaction, but also potentially destabilized the entire online car rental market for a sustained street [3].

In addition, there may be biases in the data collection process, especially when companies use historical data for forecasting, which may not fully reflect the current market environment. For example, sudden outbreaks and geopolitical events are factors that do not allow for reasonable forecasts and response scenarios to be deduced from historical data. For example, the COVID-19 epidemic had a significant impact on global supply chains, especially in the early 2020s, and many companies experienced severe inventory buildups and cash flow problems due to supply chain disruptions and unpredictable fluctuations in consumer demand. Ford Motor Company suspended production several times during the outbreak due to global chip shortages, an event that created significant uncertainty in business forecasts for the entire automotive industry, and traditional historical data could not reflect the impact of these sudden changes [3].

Another example is the impact of the UK's departure from the European Union on the intra-EU as well as the global trading system. The increase in tariffs and trade barriers after the UK's departure from the EU has caused many companies that rely on the EU market to face increased trade costs, logistical delays, and difficulties in market access. Traditional forecasting models based on historical data are inadequate in the face of such political events, and companies must adopt more flexible strategies to cope with the changing international trade environment, including finding alternative markets, reassessing supply chain networks, and investing in more market research to adapt to the new market landscape [4].

3.2. High Initial Costs

The implementation of AI requires significant initial investments in hardware (e.g., high-performance computing devices and servers), software (e.g., customized algorithms and models), and data storage and processing platforms. For small and medium-sized enterprises, the initial capital expenditure is a major barrier to AI adoption [4]. While cloud-based AI services can alleviate some of the pressure on hardware and software, long-term subscription costs can become burdensome. To some extent, AI is used more as an auxiliary tool, and the real realization of a significant improvement in the overall efficiency and profitability of the enterprise may need to go through a longer cycle, which undoubtedly increases the uncertainty and risk.

In addition to the direct costs of hardware and software, organizations need to invest in significant human resources to support the development and maintenance of AI systems. This includes hiring AI engineers, data scientists and IT support staff with specialized skills, which are also quite costly to recruit and train. Moreover, due to the rapid development of AI technology, organizations must continue to invest resources to ensure their systems and models remain up-to-date and avoid falling behind their competitors' technology, which further increases their long-term cost burden [5].

The cost of AI is also reflected in infrastructure upgrades. For example, in order to enable widespread adoption of AI, an organization's network and data storage infrastructure must be able to support high-frequency data streams and large-scale computation. This means that enterprises may need to invest in network bandwidth expansion, data center construction, and data storage capacity upgrade. For some enterprises with limited capital, these infrastructure upgrades are undoubtedly a huge financial strain.

3.3. Consumer Privacy and Data Security Issues

AI handles large amounts of consumer data in business analytics, including behavior, preferences, shopping history, and other sensitive information, which raises privacy and data security concerns. If data is not stored and handled properly, it can lead to large-scale data breaches. For example, Facebook's Cambridge Analytica data scandal in 2018 demonstrated that data misuse can have serious implications for a company's reputation and legal compliance. With the introduction of data privacy protection regulations, such as GDPR, organizations need to invest significant resources to ensure that their AI systems are compliant with privacy protection regulations. This not only increases the operational costs of organizations, but also puts higher demands on technology implementation [5]. In addition, organizations should consider following relevant ethical and compliance requirements during the development of AI systems to ensure ethical business operations and avoid legal risks [6].

4. Countermeasures

4.1. Data Governance and Optimization

In order to cope with the problem of data accuracy, enterprises must strengthen data governance to ensure the integrity and real-time nature of data. Data governance includes the standardized operation of multiple aspects of data collection, cleaning, storage, and analysis. By establishing a sound data governance framework, enterprises can effectively improve the quality of data, thereby improving the predictive and analytical capabilities of AI systems. For example, McKinsey's research points out that enterprises can significantly reduce the error of AI prediction and improve the accuracy of business decisions by improving data quality through data governance [7].

The core of data governance lies in the establishment of standardized data management processes to ensure that data remains of high quality throughout its lifecycle. Enterprises can utilize cloud-based data management platforms for real-time data updates and collaborative cross-system management to ensure data accuracy and consistency. For example, by centralizing data management across enterprise departments and establishing uniform data standards, enterprises can avoid analytical errors caused by data inconsistencies. In addition, the introduction of a data version control system can also effectively record the process of data changes and facilitate the tracing of data sources and modification history, thus improving the transparency and credibility of data [7].

In order to reduce data bias, enterprises can adopt automated data cleansing and processing tools. Data cleansing is an important part of data governance that aims to remove errors, duplicates, and incomplete information from data, thus ensuring that the data used for AI analysis is of high quality. For example, DHL has optimized the collection and analysis of logistics data through its AI system, significantly improving the accuracy and timeliness of its distribution route planning and reducing manual intervention and errors in its operations.

During the data governance process, enterprises can also consider using a master data management (MDM) system. MDM is a tool for managing core enterprise data, and by integrating and normalizing data from disparate sources, data silos can be eliminated to ensure that all parts of an enterprise use a consistent data source. For example, a large retail enterprise can unify the management of product information, customer information and supplier information through the MDM system, thereby improving data availability and accuracy and providing a more reliable data base for analysis and forecasting by the AI system.

In addition, enterprises should strengthen the real-time management of data. In order to improve the responsiveness of AI systems to market changes, enterprises need to ensure that data can be updated in a timely manner and reflect the latest market conditions. By deploying a real-time data stream processing system, enterprises can collect and analyze data at the first time it is generated, thereby improving the timeliness of decision-making. For example, financial firms can take advantage of highly volatile market conditions by monitoring market data in real time and utilizing AI algorithms to quickly make risk assessments and investment decisions.

4.2. Reducing the cost of AI technology implementation

To reduce the initial implementation costs of AI technology, organizations can employ a variety of strategies to reduce the financial burden and increase the viability of the technology. First, instead of purchasing expensive hardware and software all at once, organizations can opt for on-demand rentals of cloud-based AI services such as Amazon Web Services' AI tools or Microsoft Azure. This flexible cloud-based model enables enterprises to adjust the usage of computing resources according to actual demand, thus significantly reducing the initial investment cost, especially for small and medium-sized enterprises, and this approach can effectively lower the threshold of entering the AI technology field [8].

In addition, enterprises can also obtain AI solutions by cooperating with external technology providers. Partnering with a professional AI service company can help enterprises obtain professional technical support and customized AI models at a lower cost without having to set up a large data science team internally [8]. This on-demand access to AI services model is particularly suitable for organizations that need to apply AI technology on a small scale. For example, Shopify provides small and medium-sized e-commerce enterprises with an easy-to-integrate AI recommendation system by partnering with a third-party AI service provider, thus helping these enterprises acquire intelligent business analytics capabilities without large-scale investments.

In addition, businesses can consider participating in AI technology support programs offered by government and industry organizations. Recognizing the importance of AI technology to economic growth and competitiveness, many governments have introduced subsidies, tax incentives, and low-interest loan programs to encourage enterprises, especially small and medium-sized enterprises, to actively adopt AI technology. For example, the Digital Europe Program launched by the European Union provides financial support and technical training for SMEs to help them better utilize AI technology to enhance their competitiveness.

Enterprises can also further reduce costs by sharing AI infrastructure. For example, some industry alliances and innovation incubation centers have established AI technology sharing platforms that allow multiple enterprises to share high-performance computing equipment and data storage resources. This model can significantly reduce companies' spending on hardware facilities while promoting knowledge sharing and technology innovation within the industry. In the healthcare industry, many research institutes and hospitals share data resources and computing infrastructure by jointly establishing AI labs, thereby reducing the technology costs of individual organizations and increasing the efficiency of AI application in healthcare scenarios.

In addition, organizations can reduce financial pressure in phases through an incremental AI implementation strategy. Compared to fully deploying AI systems at once, enterprises can start with small-scale AI pilot projects in specific business segments to validate the effectiveness of the technology and gradually expand the scope of application. For example, some retailers first introduce AI prediction models in inventory management to reduce costs and waste by optimizing inventory levels, and then expand AI technology to other areas such as marketing and customer relationship management after gaining successful experience. Through AI innovation, enterprises can obtain more efficient technology application solutions and realize a good combination of technology and business models, thus reducing costs in the process of technology promotion [9].

4.3. Enhancing data privacy and security protection

To address data privacy and security concerns, organizations need to adopt multi-layered security measures to ensure that AI systems do not pose privacy leakage and security risks when collecting, storing, and processing data. First, enterprises should adopt encryption technology to protect data transmission and storage. Data encryption can effectively prevent sensitive information from being stolen or maliciously altered during transmission. The application of encryption technology can not only protect customers' personal information, but also ensure the security of confidential data within the enterprise, thus reducing the risk of data leakage [10].

Second, enterprises need to establish strict data access control mechanisms to ensure that only authorized personnel can access sensitive data. This hierarchical data access management can significantly reduce the likelihood of internal data leakage and improve data security. In addition, enterprises should use multiple authentication techniques (e.g., two-factor authentication) to enhance the protection of sensitive systems and data, thereby reducing the risk of unauthorized access [10].

In the process of data protection, enterprises should also focus on the use of data anonymization and de-identification techniques. These technologies can remove personally identifiable information from data without affecting data analysis, thus reducing the risk of privacy leakage. For example, in the healthcare industry, enterprises can use data de-identification technologies to process patient data to ensure that patient identifying information is not exposed when performing AI analysis, which improves data security and maximizes the use of the data in a compliant manner.

In addition to technological tools, organizations need to establish robust data protection policies and emergency response plans to deal with potential data security incidents. For example, enterprises can set up a dedicated data protection officer (DPO) to oversee all aspects of data protection and develop a clear emergency response plan for data leakage, so that in the event of a data leakage incident, countermeasures can be taken swiftly to reduce the negative impact on the enterprise's reputation and customer trust. Additionally, organizations should conduct regular security audits and stress tests to ensure that the security of AI systems and data storage infrastructure meets industry standards.

In terms of technology, organizations can consider using new technologies such as Federated Learning (FL) to protect data privacy. Federated Learning is a decentralized machine learning approach that allows AI models to be trained without centralizing data, thereby avoiding the risk of data sharing and privacy breaches. For example, multiple banks in the financial industry can jointly train fraud detection models through federated learning without directly sharing customer data, which protects customer privacy and improves model effectiveness. In addition, Differential Privacy can be applied to AI systems to further enhance data security by introducing random noise into the data to prevent personal information from being leaked.

5. Conclusion

AI technology offers unprecedented opportunities for business analytics to help companies optimize decision-making, reduce costs, and increase market agility. However, AI adoption also faces many challenges, including data accuracy, initial implementation costs, and consumer privacy. By strengthening data governance, reducing the initial costs of AI technologies, and implementing strict data privacy protections, organizations can better leverage AI technologies to enhance their market competitiveness and achieve long-term sustainability.

Future research can be expanded in the following areas: first, it can explore how to utilize multi-source data fusion technology to enhance AI's resilience to market changes, especially how AI can more accurately predict and provide business decision support in the face of unexpected events such as epidemics and geopolitics. In addition, research can be conducted on how to design more efficient and cost-effective AI implementations to lower the barriers to AI adoption for SMEs. Finally, for the issue of data privacy protection, further research can be conducted on how to optimize AI algorithms

using techniques such as federated learning while safeguarding data privacy, so as to achieve a balance between technology and regulatory requirements.

References

[1] J. Smith, The role of AI in business analytics, J. Bus. Res. 123 (2020) 45-58.

[2] A. Johnson, AI and its impact on emerging markets, in: Proc. Int. Conf. AI Appl., (2021) 78-89.

[3] L. Brown, M. Green, COVID-19 and supply chain disruptions, Int. J. Supply Chain Manag. 15(4) (2022) 102-115.

[4] R. Patel, The cost of implementing AI in SMEs, Small Bus. Econ. 53 (2019) 125-136.

[5] K. Williams, Data privacy in the age of AI, J. Inf. Secur. 34(2) (2018) 123-134.

[6] A. Lewis, AI and ethical business practices, Bus. Ethics J. 45(3) (2020) 112-127.

[7] McKinsey & Company, Data governance for enhanced AI performance, McKinsey Insights (2021) 54-67.

[8] P. Davis, Cloud-based AI solutions for SMEs, J. Cloud Comput. 19(3) (2020) 77-89.

[9] D. Turner, AI innovation in modern business, Global Technol. Rev. 22(4) (2021) 89-105.

[10] H. Thompson, Enhancing data security in AI systems, J. Cybersecur. 28(1) (2022) 34-45.