Journal of Computer Science and Artificial Intelligence
ISSN: 3078-8242 (Print), ISSN: 3078-2309 (Online) | Vol. 2, No. 2, 2025

Practical Applications of Large Language Models in Enterprise-Level Applications

Qianru Xu[1, *]

[1]530 Showers Dr, Mountain View, CA 94040, USA

[*]Corresponding author

Abstract: As a key achievement in the field of artificial intelligence, the Large Language Model (LLM) has great potential for development in enterprise applications. This study explores the widely used big language models and elaborates on their application capabilities in processing natural language, creating text content, and data parsing. It also analyzed the key issues that enterprises encounter when utilizing big language models, such as data security vulnerabilities, accuracy errors, system integration difficulties, and employee adaptability. A series of response strategies are proposed to address these issues, such as developing standardized frameworks, strengthening data privacy protection, conducting model refinement and validation, balancing cloud services and localized deployment, and increasing acceptance of new technologies through employee education. Provide reference and operational guidelines for enterprises to efficiently and securely implement large-scale language models.

Keywords: Big language model; Enterprise level applications; Data privacy; System compatibility; Practical Strategy.

1. Introduction

With the advancement of intelligent technology, advanced big language models have gradually become a key force in helping enterprises complete digital transformation. However, in the specific implementation process, enterprises face many challenges and difficulties, especially regarding data confidentiality, system integration, and user adaptability. How to balance innovation and potential risks, and appropriately use big language models to optimize operational processes, is an urgent problem that enterprises need to answer. This article aims to summarize the characteristics of popular big language model technologies, deeply analyze their limitations and risks in the process of enterprise application, and explore application methods with specific examples to help enterprises maximize the utility of big language models.

2. 1Introduction to Current Mainstream Language Models

The currently popular language models on the market include GPT from OpenAI, Bard from Google, LLaMA from Meta Platforms, and Claude from Anthropic, as shown in Figure 1. These advanced models all adopt deep learning principles and rely on massive datasets and neural network structures to complete pre training, demonstrating excellent language understanding and generation skills. OpenAI's GPT series, as a paradigm of LLM, is widely known for its excellent generative training features and wide adaptability, and is often applied in various scenarios such as text writing, programming assistance, and language conversion. The latest iteration of GPT-4 has significantly improved its ability to handle diverse input information and complex logic inference[1]. Bard, as a result of Google's expertise in search technology and knowledge graphs, is committed to providing precise question answering services and real-time data support. The LLaMA launched by Meta is a customizable large-scale language model feature aimed at the open source community, which has won great interest from numerous researchers and developers. Claude, developed by Anthropic, focuses on the security of conversations and the manageability of content, making him particularly suitable for situations where strict content needs to be generated.

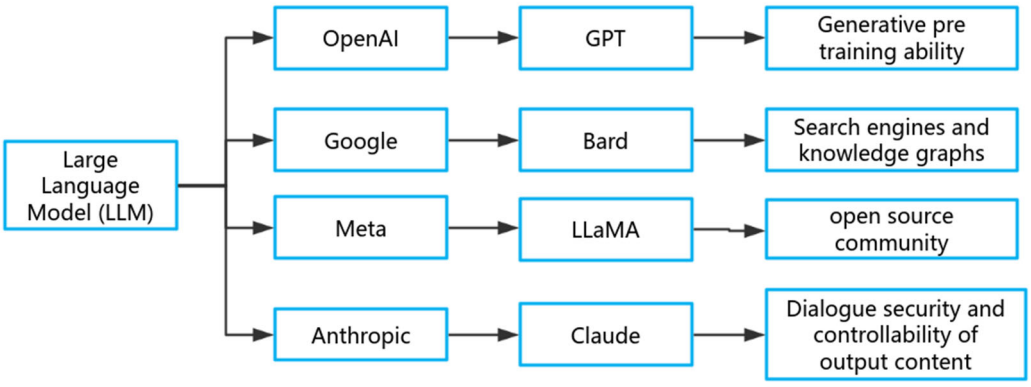

Figure 1. Common Large Language Models.

3. Problems of Large Language Models in Enterprise Applications

3.1. There is a risk of data leakage

In enterprise level applications, the data security issues involved in big language models are particularly prominent. These advanced models will come into contact with sensitive information of enterprises, such as enterprise secrets, customer privacy information, and internal operational data, when processing massive amounts of user data. In the process of interacting with these models, if sensitive information is not encrypted or transmitted through secure channels, it may be intercepted or improperly utilized. Most large language models are hosted by external enterprises and often deployed in the cloud. However, this convenient deployment model brings security risks because enterprise data must be uploaded to the hosting party's servers. If the security protection of cloud service providers is not sound enough or they encounter network attacks, critical information of enterprises may be leaked. At the same time, non-standard data storage and processing methods may also subject businesses to legal penalties, such as violating GDPR or CCPA regulations[2].

3.2. Model accuracy deviation

Although large language models can demonstrate excellent performance in many situations, accuracy errors still exist, especially in enterprise level application scenarios, where such errors can have significant negative impacts. Due to the fact that the training of these models is based on information on the network or other publicly available data sources, which may contain inaccurate information, incomplete data, or outdated content, the models may make judgments based on incorrect knowledge or provide answers that do not match actual needs when generating responses[3]. When dealing with highly specialized or relatively niche domain content, large language models may exhibit insufficient abilities. In professional fields such as finance, healthcare, and law, due to the involvement of precise terminology and rigorous logical reasoning, models may find it difficult to deeply grasp the meaning of the text and may overlook key information or make incorrect interpretations of the information.

3.3. Compatibility issues with existing enterprise systems

Ensuring system compatibility becomes one of the key challenges faced by enterprise technology governance when introducing new information modules or upgrading technologies into existing enterprise systems[4]. This problem is highlighted in the obstruction of data exchange between information systems, interface mismatch, and inconsistency of technical specifications. Some outdated systems may still use proprietary, closed data formats, while newer systems tend to be compatible with standardized, open interfaces. The following are specific issues encountered in presenting enterprise system compatibility in a table format:

Table 1. Compatibility issues of enterprise systems.

System module	Compatibility issue description	influence	Solution suggestions
ERP and CRM	There are differences in the titles of the information columns, resulting in deviations in the corresponding relationships between the fields	Information redundancy and decision-making errors	Standardize field specifications and strengthen data cleaning processes
Old SCM system	Lack of support for JSON protocol, forcing separate development of conversion layer software	R&D expenses increase, collaboration efficiency weakens	Build standardized data interfaces or adopt external conversion systems
Database compatibility	The current system uses PostgreSQL database, while the old version system is based on Oracle, and there are differences in the data storage structure between the two	Data migration is cumbersome, resulting in reduced operational efficiency	Using ETL tools and configuring for efficiency improvement
Hardware/Network Environment	The new functional module requires high hardware configuration, and current devices do not have multi-threaded computing capabilities	Slow system response and decreased stability	Update hardware facilities or migrate to cloud service solutions

Table 1 presents intuitively the challenges faced by system compatibility and their potential response strategies, indicating clear improvement paths for management.

3.4. Low acceptance of new technologies by enterprise employees

The unsuitability of employees to new technologies such as big language models has become one of the main obstacles affecting their efficient utilization. Mainly caused by employees' unfamiliarity with new technologies, difficulty in operation, and resistance to changes in work methods. Employees feel doubtful and even resistant due to a lack of understanding of the working mechanism and function of such models. They may be worried that they do not have the skills needed to adapt to new technologies, or afraid that artificial intelligence will replace their job positions, showing a negative acceptance attitude. Using a large language model requires a certain level of technical knowledge, and its interface operation, functional configuration, and operation process may be difficult for employees who are not proficient in technology to master. At the same time, the application of the model in specific scenarios (such as automatic report generation or data analysis) may disrupt employees' existing work patterns, causing them to feel uncomfortable and stressed[5].

4. Practical Strategies of Big Language Models in Enterprise Applications

4.1. Compliance Framework and Privacy Protection Measures

In the actual application scenarios of enterprises, the application and deployment of big language models need to take compliance as the core criterion to ensure that information privacy and security are not violated. Building a compliance architecture is a fundamental requirement for enterprises at the application level. Following relevant laws, industry standards, and ethical norms can help reduce legal litigation risks and trust issues. Confidentiality measures are crucial for ensuring the security of user data, ensuring that sensitive information is not leaked or illegally exploited during processing and storage. The company should establish a comprehensive compliance management framework to comprehensively supervise the entire process of data collection, storage, transmission, processing, and deletion. The main legal basis involved in this is the General Data Protection Regulation (GDPR), the Personal Information Protection Law (PIPL), etc. For example, in the process of information collection, enterprises should clearly explain the intended use of the data to users and obtain their explicit consent. The storage and transmission of data should use encryption technology, set up firewalls and other security measures.

In the field of maintaining privacy and security, differential privacy and federated learning have become two key technologies[6]. Differential privacy ensures that personal information is not individually identified by introducing random noise into the data, while federated learning technology achieves decentralized processing of data by training models on local devices, reducing the possibility of data leakage. For the compliant application of big language models, technical measures are only one aspect, and corresponding policy support and implementation are equally indispensable. It is necessary to establish detailed data utilization standards and enhance employees' awareness of regulatory compliance through training. When collaborating with external partners, signing strict data confidentiality contracts is also an important step in ensuring the privacy protection of the entire supply chain. Taking a certain online customer service company as an example, the company optimized the customer service process using a big language model. The company has adopted federated learning methods, effectively avoiding direct transmission of customer data to central servers and reducing the risk of data leakage. The enterprise adopts the following formula to evaluate the balance between privacy risk and accuracy of the model:

$$P = E - \frac{\lambda}{n} \tag{1}$$

In formula (1), P represents the level of privacy protection, E represents the model accuracy, λ represents the disturbance intensity, and n represents the number of devices participating in federated learning. Experiments have shown that when λ is appropriately increased, user privacy is improved while the loss of model accuracy is acceptable.

4.2. Model tuning and validation

In practical application scenarios of enterprises, tuning and validating large language models is an important step. Optimization work involves optimizing the hyperparameters, training methods, and data preprocessing techniques of the model, with the aim of enhancing its functionality. The verification phase focuses on using multiple evaluation methods to confirm the stability and accuracy of the model in practical operation. The initial stage of optimization is the selection of pre trained models. Generally speaking, large language models rely on massive unlabeled text data for pre training. Enterprises can choose suitable benchmark models according to their specific needs, such as GPT or BERT. Subsequently, the hyperparameters of the model were finely adjusted, including learning rate, batch size, network layers, and the number of hidden nodes. Accurate control of these parameters can enable the model to demonstrate superior generalization ability and predictive effectiveness in various tasks[7]. In addition, to meet the customized needs of enterprise scenarios, optimizing the model also involves creating a dedicated training dataset and applying data augmentation strategies. In order to evaluate the accuracy of the model, cross validation, A/B testing, and other methods will be used to test the reliability and stability of the model in various contexts. In the sales forecasting scenario of enterprises, they use past sales data to train forecasting algorithms and predict the sales trend for the next few months. By adjusting the model and optimizing its parameter settings based on the characteristics of sales data, it can more accurately reflect factors such as seasonal fluctuations and promotional activities. For example, considering the uniqueness of time series data, strategies such as ARIMA models may be adopted to enhance the predictive performance of large-scale language models. Combining complex mathematical formulas in this process can help describe the predictive ability of the model. Assuming the output of the model is yt, the following formula can be used for prediction:

$$y_t = \alpha \cdot y_{t-1} + \beta \cdot X_t + \varepsilon_t \tag{2}$$

In formula (2), y_t is the predicted value at the current time, y_{t-1} is the actual value at the previous time, Xt is the external feature at the current time (such as promotional data, market volatility, etc.), αand β are the coefficients of the model, representing the degree of influence of autoregression and external factors, and ϵ_t is the error term. By adjusting the model parameters, it helps to enhance the accuracy of predictions, allowing large language models to output more precise prediction results when analyzing complex enterprise information.

4.3. Selection of Cloud and Local Deployment

In the application process in the enterprise field, deciding whether to deploy the big language model in the cloud or on premises is a core decision that requires a comprehensive evaluation of cost-effectiveness, operational efficiency, data security, and scalability. Cloud deployment is favored by many enterprises due to its flexibility and convenience. Cloud service providers provide pre-set model interfaces for enterprises to quickly achieve integration and scale expansion. Cloud deployment can dynamically adjust computing resources according to changes in business needs, reducing the initial investment of enterprises in infrastructure. However, there are also some shortcomings in cloud deployment, such as potential latency issues and security risks

in data transmission, especially in scenarios where sensitive data is processed, which may face the risk of data leakage[8].

In contrast, local deployment can better control data privacy and model performance. In the local environment, enterprises can directly manage data flow and avoid uploading sensitive information to third-party platforms. This deployment method is particularly suitable for applications that require rapid response, as all data processing and model inference are completed within the local network, reducing the risk of network latency. However, this deployment method also has its shortcomings, namely high upfront hardware investment and sustained maintenance burden. Especially for large language models that require a large amount of computing resources, enterprises must equip themselves with high-end hardware facilities, such as high-efficiency GPUs or TPUs. A medical unit has implemented a hybrid deployment plan to intelligently process patient medical information. The unit processes patient data that involves privacy locally, while handing over statistical analysis work that does not involve privacy to the cloud for processing. The hospital has optimized the allocation formula for data flow and designed the following decision model based on data sensitivity and computational requirements:

$$S = \alpha \cdot C_{cloud} + \beta \cdot C_{local} + \gamma \cdot D_{security} \quad (3)$$

In formula (3), S is the comprehensive score, C_{cloud} and C_{local} represent the computational costs of cloud and on premises deployment, $D_{security}$ is the security weight, and α, β, and γ are the adjustment coefficients. Through fine tuning of parameters, the company has successfully improved computational efficiency by 40% and ensured data security. This successful case provides valuable theoretical support and practical operational reference for other companies in the same industry in similar decision-making and implementation processes.

4.4. Enterprise organization employee training and skill enhancement

In the process of integrating big language models into enterprise operations, enhancing employee skills is one of the core aspects. It is necessary to rely on standardized training to ensure that employees can proficiently master relevant technologies and effectively apply models, bringing maximum benefits to the organization. Training should focus on two dimensions: technical proficiency and business application skills. Technical proficiency mainly targets the technical department, helping employees master the core concepts, usage processes, and optimization techniques of the big language model. This training content includes model structure analysis, data preprocessing methods, parameter adjustment strategies, API usage instructions, etc.

For non-technical personnel, business skill enhancement training is dedicated to enabling them to master the practical application of big language models. Customer service personnel in enterprises need to master the skills of using models to promote communication with customers, while marketing teams need to be familiar with data analysis tools that rely on models in order to predict consumer behavior and plan marketing strategies. Taking a manufacturing company that uses a big language model to optimize its supply chain as an example, the company has implemented targeted education for its employees, including training on the basic principles and specific operational steps of the model. The following is a data analysis table of the training effectiveness of the enterprise:

Table 3. Training Effect Display Table.

Training phase	Number of participants	Average test score (out of 100)	Actual application rate	Work efficiency improvement rate
Before training	50	45	10%	-
After primary training	50	75	50%	20%
After advanced training	50	90	85%	35%

According to the data in Table 3, it can be seen that systematic education enhances employees' professional skills and work efficiency. This proves that adopting efficient training methods can enhance employees' ability to apply large-scale language models, accelerate the application of these abilities to specific business operations, and promote the completion of digital transformation and upgrading of enterprises.

5. Conclusion

Large language models are demonstrating their disruptive impact in enterprise applications. But the full realization of its potential depends on enterprises tailoring corresponding strategies based on specific needs and potential risks. From a technical perspective, compliance, data privacy security, optimization and upgrading of models, and selection of deployment strategies are crucial. In terms of organizational dimension, the skill development and technical acceptance of staff should not be underestimated. With the continuous advancement of modeling technology and the enrichment of industry application practices, big language models have the potential to become a key tool for enterprises to enhance their competitiveness and innovation capabilities. On the premise of ensuring data security and application efficiency, enterprises should actively explore its potential value to cope with the challenges of digital transformation.

References

[1] Ge Jin, et al."A comparison of large language model versus manual chart review for extraction of data elements from the electronic health record.."Gastroenterology 166.4(2023):707-709.e3.

[2] Rathi H., et al."P21 A Comparative Analysis of Large Language Models (LLM) Utilised in Systematic Literature Review."Value in Health 26.12S(2023):S6-S6.

[3] Birkun Alexei A,and Gautam Adhish."Large Language Model (LLM)-Powered Chatbots Fail to Generate Guideline-Consistent Content on Resuscitation and May Provide Potentially Harmful Advice.."Prehospital and disaster medicine 38.6(2023):1-7.

[4] Pal Soumen, et al."A Domain-Specific Next-Generation Large Language Model (LLM) or ChatGPT is Required for Biomedical Engineering and Research.."Annals of biomedical engineering 52.3(2023):451-454.

[5] Ryan Watkins."Guidance for researchers and peer-reviewers on the ethical use of Large Language Models (LLMs) in scientific research workflows."AI and Ethics 4.4(2023):969-974.

[6] Perera Molligoda Arachchige Arosh S."Large language models (LLM) and ChatGPT: a medical student perspective.."European journal of nuclear medicine and molecular imaging 50.8(2023):2248-2249.

[7] Naik Himani R,Prather Andrew D,and Gurda Grzegorz T."Synchronous Bilateral Breast Cancer: A Case Report Piloting and Evaluating the Implementation of the AI-Powered Large Language Model (LLM) ChatGPT.."Cureus 15.4(2023):e37587-e37587.

[8] Alberts Ian L, et al."Large language models (LLM) and ChatGPT: what will the impact on nuclear medicine be?."European journal of nuclear medicine and molecular imaging 50.6(2023):1549-1552.