WHITE PAPER

EDGE BRICKS

What is EdgeBricks ?

Edgebricks empowers businesses by offering a comprehensive and scalable solution, ensuring that AI/ML projects have the necessary infrastructure to thrive.
Machine learning infrastructure serves as a crucial necessity for any AI/ML project within an organization. At Edgebricks, we strive to simplify the process by offering an intuitive and user-friendly infrastructure solution, specifically designed for building and managing AI/ML workloads.

Explain the concept of AI.

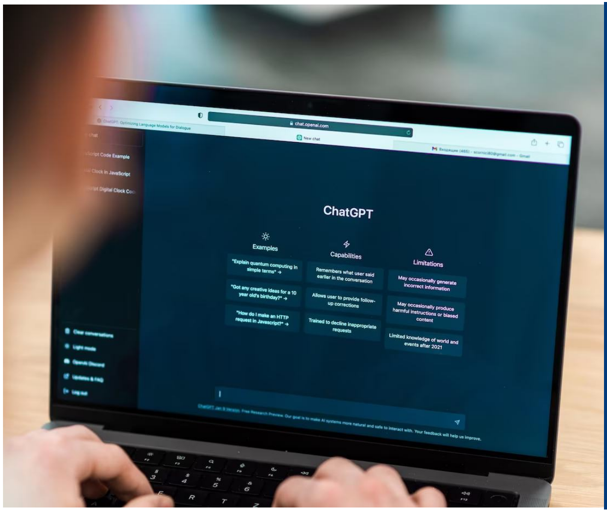
AI, or Artificial Intelligence, is a field of computer science that focuses on creating systems and machines capable of performing tasks that would normally require human intelligence. The ultimate goal of AI is to develop machines that can mimic and simulate human cognitive processes, such as learning, reasoning, problem-solving, perception, language understanding, and decision-making.

Overcoming Data Privacy Challenges in Developing Proprietary Chatbots

www.edgebricks.com

Introduction

This whitepaper delves into the challenges companies face when developing chatbots using their own data, with a primary focus on data privacy. In today's business landscape, integrating chatbots is crucial for enhancing customer engagement and operational efficiency. However, ensuring data privacy while leveraging proprietary data presents a significant hurdle.



Challenges Faced

Despite the promises of various LLMs like OpenAI, Claude, Facebook’s LLama, Google Gemini companies encounter several challenges in effectively harnessing their potential for chatbot development.
These challenges are outlined as follows:

Data Security and Privacy

Handling sensitive financial data raises concerns regarding data security, compliance with regulatory standards (such as GDPR and CCPA), and protecting customer privacy. Most SaaS based solutions ask you to upload your data to their systems to help you build a chatbot. This is a non-starter for most enterprises.

Automating Complete Chatbot Lifecycle Management

Handling sensitive financial data raises concerns regarding data security, compliance with regulatory standards (such as GDPR and CCPA), and protecting customer privacy. Most SaaS based solutions ask you to upload your data to their systems to help you build a chatbot. This is a non-starter for most enterprises.

Training Time and Resources

Building your own LLM with your data requires significant computational resources and time, which can be a challenge for companies with limited resources. This forces them to evaluate other approaches like RAGs and fine tuning foundational models that are available.

Maintenance and Updates

Keeping the chatbot up-to-date with the latest model versions and improvements from the open-source community requires ongoing maintenance efforts.

User Acceptance Testing

Ensuring the chatbot meets user expectations and provides a satisfactory user experience requires rigorous testing, which can be resource-intensive.

Scalability

As user demand grows, scaling the chatbot's infrastructure to handle increased traffic and interactions can be challenging without proper planning.

Chatbot access to internal systems and databases

Seamless integration enabling chatbot access to internal systems and databases. Efficiently integrating chatbots with internal systems and databases for streamlined data access and interaction is a challenge.

Regulatory Compliance

Financial and other institutions must adhere to stringent regulatory requirements like PCI DSS, NIST, HyTrust, HIPAA and other data protection laws, which necessitate compliance mechanisms within chatbot systems.

```
<html>
<head>
<script>
function show(shown, hidden) {
  document.getElementById(shown).style.displ
  document.getElementById(hidden).style.displ
  return false;
}
</script>
</head>
<body>

  <div id="Page1">
    Content of page 1
    <a href="#" onclick="return sh
```

Edgebricks: Secure and compliant chatbot

Edgebricks offers a unique solution for developing and deploying chatbots. Addressing the challenges and capitalizing on the opportunities presented by conversational AI. The key features that set Edgebricks apart include:

Hosting in customer accounts

With Edgebricks, chatbot development is simplified, requiring no technical expertise. Users can upload data, select embedding techniques, customize language models, and deploy chatbots within minutes

Built in development lifecycle

With Edgebricks, chatbot development is simplified, requiring no technical expertise. Users can upload data, select embedding techniques, customize language models, and deploy chatbots within minutes

Feedback Loop

The platform includes automated quality assurance mechanisms that streamline the testing and validation process, saving time and resources while ensuring the reliability and accuracy of the chatbots.

Built in QA automation

Building your own LLM with your data requires significant computational resources and time, which can be a challenge for companies with limited resources. This forces them to evaluate other approaches like RAGs and fine tuning foundational models that are available.

Scalable deployment

The platform supports batch mode processing, enabling the seamless handling of multiple queries simultaneously. This feature enhances the scalability and efficiency of chatbot deployments, ensuring smooth operations even during peak demand periods.

Use Cases

We handle various different use cases for our customer while building the chatbot. Some of these include:

Enhanced Customer Experience

Chatbots enable round-the-clock assistance, personalized recommendations, and seamless handoff to a real human, enhancing the overall customer experience.

Operational Efficiency

Automating routine inquiries, such as balance inquiries, transaction history, and account management, streamlines operations and reduces operational costs.

Sales and Marketing

Chatbots serve as virtual assistants, guiding users through product offerings, assisting with onboarding processes, and facilitating cross-selling opportunities.

Healthcare

Chatbots tailored for healthcare, aiding in patient engagement, appointment scheduling, and telemedicine support while ensuring HIPAA compliance.

Finance

Chatbots for the finance industry can assist with customer support, account management, and fraud detection, all while maintaining stringent security measures.

Retail

Retailers can utilize chatbots for personalized shopping assistance, product recommendations, order tracking, and inventory management, driving sales and enhancing customer satisfaction.

Hospitality

Chatbots can be used to develop chatbots for hotel booking assistance, concierge services, and guest inquiries. These chatbots can provide personalized recommendations, handle reservations, and address customer queries promptly, enhancing the guest experience and improving operational efficiency.

Conclusion

Gen AI chatbots are becoming very common across the enterprises to solve various business needs, optimize processes and improve productivity of their teams. However, building one using existing base LLMs and private data is not a simple task. One needs to solve various challenges in going from development to production deployment

Edgebricks has built a complete chatbot lifecycle management platform that simplifies development, testing and deployment, enabling organizations to enhance customer engagement and satisfaction through conversational AI.

We solve the biggest challenges in data privacy and compliance by offering a deployment approach within a customer's account using cloud-agnostic hosting. Please reach out to us at www.edgebricks.com for more information.

Thank You

EDGE BRICKS

Empowering AI & LLM Innovation

Contact Us:
(650) 204-9027

Email:
info@edgebricks.com

www.edgebricks.com