Patent Search

Invention Title	A Zero-Exposure Architecture for Secure AI Interaction
Publication Number	20/2026
Publication Date	15/05/2026
Publication Type	INA
Application Number	202641057350
Application Filing Date	06/05/2026
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMPUTER SCIENCE
Classification (IPC)	G06F 21/62, G06F 21/60, G10L 15/22, G10L 15/18, G06N 3/04

Inventor

Name	Address	Country
Dr. V. S. N. Narasimha Raju	Professor, Department of EEE, Vishnu Institute of Technology, Sri Vishnu Education Society, Vishnupur, Bhimavaram, Andhra Pradesh 534202	India
Dr. Rangarao Orugu	Associate Professor, Department of ECE, Vishnu Institute of Technology, Sri Vishnu Education Society, Vishnupur, Bhimavaram, Andhra Pradesh 534202	India
G. Surya Teja	Student, Department of CSE, Vishnu Institute of Technology, Sri Vishnu Education Society, Vishnupur, Bhimavaram, Andhra Pradesh 534202	India
B. NAGAMALLIKA	Student, Department of CSE, Vishnu Institute of Technology, Sri Vishnu Education Society, Vishnupur, Bhimavaram, Andhra Pradesh 534202	India
SK. MAHAB JAN	Student, Department of CSE, Vishnu Institute of Technology, Sri Vishnu Education Society, Vishnupur, Bhimavaram, Andhra Pradesh 534202	India
A. SITA RATHNAM	Student, Department of AIML, Vishnu Institute of Technology, Sri Vishnu Education Society, Vishnupur, Bhimavaram, Andhra Pradesh 534202	India
CH. HEMANTH	Student, Department of AIML, Vishnu Institute of Technology, Sri Vishnu Education Society, Vishnupur, Bhimavaram, Andhra Pradesh 534202	India
K. BHANU VIVEK	Student, Department of IT, Vishnu Institute of Technology, Sri Vishnu Education Society, Vishnupur, Bhimavaram, Andhra Pradesh 534202	India

Applicant

Name	Address	Country
Vishnu Institute of Technology	Vishnu Institute of Technology, Sri Vishnu Education Society, Vishnupur, Bhimavaram, Andhra Pradesh 534202	India

Abstract:

The present disclosure relates to systems and methods for privacy-preserving interaction with large language models, and provides a Zero Exposure Architecture (10 to operate as a dual-channel privacy mediation system positioned between the user and the large language model, intercepting user input and processing each categ separate coordinated pathways. The Zero Exposure Architecture (100) includes a sensitivity classification engine (104) that partitions user input into non-sensitive and streams, an encoding module (110) that replaces sensitive values with placeholder tokens (112) stored in ephemeral session memory (114), and a decoding module (reconstructs the response prior to delivery. This configuration ensures sensitive information is never directly exposed to the large language model, shifting privacy pr from policy-based trust to architectural enforcement.

Complete Specification

Description:TECHNICAL FIELD

[001] The present invention relates to artificial intelligence systems and data security, and more particularly to a Zero Exposure Architecture for privacy-preserving interaction with large language models, wherein sensitive user information is detected, isolated, and replaced prior to transmission to any external AI model.

BACKGROUND

[002] The field of artificial intelligence systems and data security has witnessed considerable growth with the widespread deployment of large language models acr industries including banking, healthcare, education, legal services, and customer support. These models are typically accessed through application interfaces that re natural language prompts from users, process them through external computational systems, and return contextually relevant responses. Such interactions have substantially transformed the manner in which individuals and organizations seek information, automate workflows, and engage with digital services.

[003] In conventional AI interaction systems, raw user input is transmitted directly to the large language model without any intermediate analysis or transformation in the ordinary course of interaction, frequently include within their prompts sensitive categories of information such as personal identification numbers, financial a details, health records, contact information, and confidential organizational data. This transmission of unprocessed input to external AI systems introduces substan data security risks that may not be adequately addressed by existing architectural arrangements.

[004] Existing approaches to data privacy in AI deployments typically rely upon policy-based assurances, contractual representations by service providers, and regul compliance declarations. While such measures may offer a degree of procedural protection, they do not structurally prevent sensitive information from reaching th model itself. The confidential data, once transmitted, may be susceptible to unauthorized data logging, unintended retention in system caches, exposure through th

View Application Status

Page last updated on: 26/06/2019