Macao Funding Scheme for Key R&D Projects 2024
Application Guideline for Projects of Digital Technology (Cybersecurity)

I. Background

Cybersecurity is a crucial topic in the digital era. It not only concerns national security, social security, and information security but relates to every citizen's daily life. The "*14th Five-Year Plan*" emphasizes "improving the capabilities of cybersecurity threat detection, monitoring and early warning, emergency command, and attack traceability. We should foster the R&D of key cybersecurity technologies to accelerate the innovation of artificial intelligence security technology, thus enhancing the comprehensive competitiveness of the cybersecurity industry". The *"14th Five-Year Plan" for National Informatization* states that "security is the premise of development, and development is the guarantee of security. To build a solid defense line for data security, we should first promote classified and hierarchical management of data and ensure data is used and shared safely".

The Macao SAR Government prioritizes improving the cybersecurity capabilities. In the *Second Five-Year Plan for Economic and Social Development of the Macao Special Administrative Region (2021-2025)*, it is clearly stated that "an overall cybersecurity development strategy shall be formulated to strengthen the protection of critical infrastructure information systems and networks". The *Policy Address for the Fiscal Year 2024* proposes to "optimize cybersecurity construction to

continuously improve the level of response to cybersecurity risks and incidents".

In order to further integrate the existing superior resources and enhance Macao's cybersecurity technology capabilities, the Science and Technology Development Fund (FDCT) has proposed this Scheme for Key R&D Projects after taking into opinions and suggestions from Macao's researchers in relevant fields and seeking expertise from mainland experts. It aims to help Macao bring its strengths into full play in a planned and step-by-step manner to accommodate the needs of the country, and build a solid defense line for Macao's cybersecurity with scientific and technological innovation according to Macao's economic and social development status and needs. As a result, the protection of national security could be stepped up.

II. Overall Objectives

Under the current complex cybersecurity situation, it aims to guarantee various tasks related to cybersecurity, keep containing cyberattacks to continuously improve the security of information networks and computer systems, and improve the intelligent protection capability in the field of information security. Therefore, the defense line for Macao's cybersecurity could be consolidated.

III. Research Field

Research field: Research and application of modeling technology of large language models (LLMs) for information security

(1) The modeling methods of LLMs in the vertical field of information security. The LLM fine-tuning and

lightweight deployment of LLMs for information security should be studied to solve the problems of low accuracy and high costs of LLM threat analysis and processing in the field of information security.

(2) The methods for automated generation of datasets. The research should focus on automated dataset generation methods for LLMs in the field of information security, including data cleansing and preprocessing, dynamic processing of data, and intelligent enhancement methods of data in the field of information security to form high-quality datasets and automated generation systems in the field of information security.

(3) The building methods of AI agents. The AI agent construction method based on LLMs in the field of information security should be studied to create agents such as multi-source heterogeneous alarm data fusion, alarm evaluation and attack analysis, threat intelligence extraction, abnormal behavior analysis, and network red team intelligent attack drills.

(4) The security enhancement methods of AI agents. The methods of hallucination detection, defense against poisoning attack, and adversarial example defense should be studied.

(5) An intelligent service platform oriented to the field of information security should be researched and developed. The platform is applicable in various scenarios such as intelligent Q&A, attack detection and defense, and secure operation.

Performance indicators:

(1) A large model in the field of information security is

built.

(2) A large-scale cybersecurity knowledge base covering assets, vulnerabilities, attacks, and other dimensions is established. The built cybersecurity knowledge base has 1 billion entries with no less than 5 types of integrated multi-source heterogeneous alarm data.

(3) The accuracy of AI agent alarm and attack behavior mapping is greater than 85%, the accuracy of threat intelligence extraction reaches 90%, the detection accuracy against typical Web attacks is greater than 90%, and the classification accuracy of network traffic is greater than 95%.

(4) Defense against at least 5 kinds of poisoning attacks; under the existing adversarial example attacks, the detection and classification accuracy is reduced by no more than 10%; the detection accuracy for output illusion is greater than 85%.

(5) An AI agent platform is built. The platform includes scenario functions such as multi-source heterogeneous alarm data fusion, alarm evaluation and attack analysis, threat intelligence extraction and detection, and abnormal behavior analysis. A single threat event’s average endless loop processing time is less than 20 seconds.

(6) The Technology Readiness Level (TRL) shall achieve TRL 7.

IV. Application Requirements

(1) The lead applicant shall be a Macao entity, and the project shall be led or participated by enterprises,

which shall provide supporting funds of no less than 50% of the FDCT fund. If an enterprise participates in the project, it shall be a Macao or Hengqin enterprise.

(2) A formal cooperation agreement shall be provided if the project is collaborative.

(3) The project duration is 3 years. The maximum application amount for each project is MOP 15 million.

V. Experts Involved in the Formulation of the Guideline

Li Dan	Professor of Tsinghua University
Zhang Weizhe	Professor of Harbin Institute of Technology
Li Hongwei	Professor of University of Electronic Science and Technology of China
Weng Jian	Professor of Jinan University
Dong Changyu	Professor of Guangzhou University