Opportunity Title: Secure Computing and Using Homomorphic Encryption for Machine Learning on Sensor Data and Privacy Fellowship
Opportunity Reference Code: ICPD-2024-49

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2024-49

How to Apply **Create and release your Profile on Zintellect** – Postdoctoral applicants must create an account and complete a profile in the on-line application system. **Please note: your resume/CV may not exceed 3 pages.**

Complete your application – Enter the rest of the information required for the IC Postdoc Program Research Opportunity. The application itself contains detailed instructions for each one of these components: availability, citizenship, transcripts, dissertation abstract, publication and presentation plan, and information about your Research Advisor co-applicant.

Additional information about the IC Postdoctoral Research Fellowship Program is available on the program website located at: https://orise.orau.gov/icpostdoc/index.html.

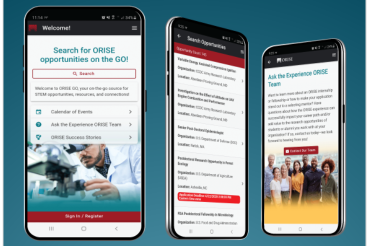
If you have questions, send an email to ICPostdoc@orau.org. Please include the reference code for this opportunity in your email.

Application Deadline 2/28/2024 6:00:00 PM Eastern Time Zone

Description **Research Topic Description, including Problem Statement:**

The concern and need to protect data and privacy continue to grow. Over the years, fully homomorphic encryption (FHE) has emerged as a possible solution and offers defense mechanisms that allows computations to be performed directly on encrypted data while maintaining confidentiality. However, high computational complexity on large ciphertexts had limited the capability for FHE to be leveraged. To address these challenges, there is a need for cryptographic accelerators that can expedite real-world application deployment. Thus, the objective of this project is to design and optimize the homomorphic encryption algorithm to enhance data sharing and confidentiality. To accomplish the research objective, there is a need to develop a framework that leverages the benefits of homomorphic encryption (HE), and machine learning (ML), to protect information during data collection and sharing process against potential attacks such as data collected from supervised devices such as sensors, network flow, and camera systems that are encrypted using HE schemes. Machine learning (ML) as a cloud-based service is growing rapidly and the growth of Internet-of-Things data have given rise to a significant concern for monitoring systems while maintaining the security of data during ML inferences. Cryptographic accelerators may reduce the computational burden of homomorphic functions, enabling faster and more efficient computations on the encrypted data. The proposed approach will advance new theories and methods for effective and efficient defense processes involving homomorphic encryption, ML, and optimization of data sharing and privacy.

Additionally, how can the IC or other groups with sensitive data work (e.g., DoD, personal medical data, census data) with the data and perform advanced analyses while the data is in a protected state (i.e., encrypted). Current methods can have unacceptably large overheads and are clumsy to program, at best with their current tools working at what amounts to a gate


Welcome!
Search for ORISE opportunities on the GO!
Search
Calendar of Events
Ask the Experience ORISE Team
ORISE Success Stories
Sign In / Register
Search Opportunities
Ask the Experience ORISE Team

level of programming. It is often difficult to specify security requirements (i.e., who gets to see what data) at a fine-grained level.

Example Approaches:

(1) Develop a software architecture for integrating FHE into networks to collect data from devices such as sensors and sensing and camera systems. (2) Provide a proof-of concept by developing a small data base using the software architecture. (3) Implement the software design using simulated or real sensor arrays feeding FHE data to an encrypted data base where ML operations will be executed. (4) Deliver a report that compares the results to the same data created in an unencrypted environment and demonstrates essential equivalence of the machine learning process and outcomes. (5) prepare a user-friendly set of tools and rules to apply homomorphic encryption to the problem of machine learning and privacy preservation. (6) Explore how the FHE will perform at scale with large datasets/changing of resources and demand on the system.

Also, current techniques fully homomorphic encryption currently applies for the underlying encrypted operations, but these need to be combined with boutique programming languages and associated compilers, along with development of “data independent algorithms”. In addition, advanced security sensitive programming languages might be able to use specially developed type systems to specify data security requirements in a fine-grained way.

Relevance to the Intelligence Community:

Cyber - Develop/enhance capabilities to identify and protect critical assets, information systems, technologies, industries, and people.
Category Zero; Develop/enhance capabilities to quickly identify deception techniques.

Key Words: Homomorphic Encryption, Machine Learning, Internet of Things, Sensors, Privacy of Data, Private Information Retrieval, Oblivious RAM

Qualifications

Postdoc Eligibility

- U.S. citizens only
- Ph.D. in a relevant field must be completed before beginning the appointment and within five years of the appointment start date
- Proposal must be associated with an accredited U.S. university, college, or U.S. government laboratory
- Eligible candidates may only receive one award from the IC Postdoctoral Research Fellowship Program

Research Advisor Eligibility

- Must be an employee of an accredited U.S. university, college or U.S. government laboratory
- Are not required to be U.S. citizens

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
  - **Chemistry and Materials Sciences** (12 👁)
  - **Communications and Graphics Design** (3 👁)
  - **Computer, Information, and Data Sciences** (16 👁)
  - **Earth and Geosciences** (21 👁)
  - **Engineering** (27 👁)
  - **Environmental and Marine Sciences** (14 👁)
  - **Life Health and Medical Sciences** (45 👁)
  - **Mathematics and Statistics** (11 👁)
  - **Other Non-Science & Engineering** (2 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)
  - **Social and Behavioral Sciences** (30 👁)