Partnering Opportunity

Profile status : Published

Research Development Request

Partners dealing with AI, Robotics, 5G, IoT, Big Data or Mobile Application are sought for a project under EIC-FTI-2018-2020 Call

Summary

A Turkish SME is developing a project under H2020 Fast Track to Innovation: Simple, Stable, Secure High-Performance Computing. The project aims to to handle huge IoT data with this environment and provide a stable and robust HPC platform for the required analysis. The SME is looking for partner/s dealing with AI, Robotics, 5G, IoT and Cellular IoT, Big Data and Mobil Application.

Creation Date	04 September 2020
Last Update	23 September 2020
Expiration Date	02 October 2020
Reference	RDTR20200826001
Public Link	https://een.ec.europa.eu/tools/services/PRO/Profile/Detail/736e6796-a200-4d01-b142-017c210676b7

Details

Description

The security objective for High-Performance Computing (HPC) is not well defined with modern standardizations. Moreover, HPC system hardware support is not flexible with current environments. Configurable hardware firmware supports not meet with COTS (Commercial off-the-shelf) devices. At this point, the Turkish SME proposes a fully configurable and extendible environment with HSM (hardware security module) support for HPC applications with security features on both host and client sides. Additionally, the SME offers this security feature with AI support. This project scope about a trade-off between performance and security with intelligence way.

The security perspective of legacy systems always run with rule-based monitoring algorithms and thresholds trigger events. This project proposes a new attitude to system security for HPC environments. It considers the post-disaster effect on system users and components with AI-based effective protection modeling with high-speed cryptographic operation instruments such as HSM. HSM features are virtualizing with an additional layer and can easily multiple with the virtualization layer. HSM also can be customized for HPC specific operations via the virtualization layer. In this project, the Turkish SME will provide data-in-use, data-at-rest, and data-in-transit protection with runtime application self-protection approach with white-box cryptography and secure element features. They target dynamic threat modeling and use these models as a service to provide a dynamic system and end-point security.
The first step in the project is to focus on IoT and Cellular IoT secure communication, fast authentication, and fast revocation with AI-based anomaly detection and response features. It is aimed to handle huge IoT data with this environment and provide a stable and robust HPC platform for the required analysis. This project will be alive with data, and more data training will provide more security and more performance for the installed platform. HPC platform hardware acceleration requirement dynamically is provided with the HSM pool. HSM firmware and features can be configured and updated via the secure control layer. The HSM that offered for this project is configurable for cryptographic or other specific operations with firmware support. Also, pre-loaded firmware with lots of features can maintain market demand.

4-5 partners are sought for the proposal. The required expertise topics are Security, HPC, AI, IoT and, Robotics.

The project is divided into several work-packages; the Turkish SME has expertise in hardware and software security solutions. In this project, they will extend their solutions to the IoT, Robotic, Health, and Automotive segment. Thus, they need an IoT or Robotic expert company to work on IoT end-points as a client.
Also, the rule-based or threshold-based security approach is to be improved with AI support for anomaly detection and forecasting. Also, in this project, there will be many data to analyze AI expert companies should handle analysis. Besides, IoT and Robotic partners can need AI expertise for autonomous operations. As a platform, DecSecOps management is required for the pilot operations, and a partner can handle all this development and deployment site management. The case study can be a public health monitoring platform, and in this case study, we should provide GDPR (General Data Protection Regulation) requirements and real-time analysis. Also, there can be robots and hand-terminals for health monitoring. Also, mobile devices and wearables can be integrated with this platform.

The EoI Deadline is 2 October 2020, since the call deadline is 27 October 2020.

Advantages and innovations

3-factor strong authentication (something you own, something you know and something you are) trends will be key features to protect end-user or entities. Multiple sources will use for authentication methods such as password, device authentication, SMS, IP-geolocation, soft-OTP, device certificates, smartcards, biometrics, and more. AI-based engines will manage behavior analysis and rank-based feature management. Sensitive assets are securely stored on the clients' and hosts' environments. Zero-trust environment security is the major requirement and target for this project. All methods used to protect data on both client and host side will frequently be updated according to state-of-art threats and attack models.
The project will also offer easy integration features for most environments to make deployments and installation fast and easy. In real scenarios, we can install our security platform for industrial IoT systems, military protection systems, hospital health, and monitoring system or banking system for mobile devices. We can train real cases and create realistic models for end-user and entity activity detection. These models can be merged and used for each other to provide a robust, secure environment for all systems.
In this project, the Turkish SME offers to build intelligence security environments for HPC that can adapt to threats, forecast the risk, test itself, and partly recover installed platform. This project synchronizes all security entities with artificial intelligence support for HPC.

Technical Specification or Expertise Sought

4-5 partners are sought for the proposal. The required expertise topics are Security, High Performance Computing (HPC), Artificial Intelligence (AI), Internet of things (IoT) and Robotics.

Stage of development

Proposal under development

Keywords

Technology

01003003	Artificial Intelligence (AI)
01003009	Data Protection, Storage, Cryptography, Security
01003010	Databases, Database Management, Data Mining
01003018	User Interfaces, Usability
01003025	Internet of Things

Market

02007004	Program development tools/languages
02007016	Artificial intelligence related software

NACE

J.62.0.1	Computer programming activities

Network Contact

Issuing Partner

ZACHODNIOPOMORSKI UNIWERSYTET TECHNOLOGICZNY W SZCZECINIE

Contact Person

ZEBROWSKI Pawel

Phone number

+48 91 449 43 64

Email

pzebrowski@zut.edu.pl

Open for EOI: Yes

Client

Type and Size of Organisation Behind the Profile

Industry SME 50-249

Year Established

2013

Already Engaged in Trans-National Cooperation

Yes

Languages Spoken

Turkish
English

Client Country

Turkey

Partner Sought

Type and Role of Partner Sought

4-5 partners experienced in AI, IoT,Cellular IoT, 5G and Authentication are sought.

Type and Size of Partner Sought

SME 11-50,University,R&D Institution,SME <10,SME 51-250,>500

Type of Partnership Considered

Research cooperation agreement

Program - Call

Framework Program

H2020

Call title and identifier

EIC-FTI-2018-2020- Fast Track to Innovation

Submission and evaluation scheme

Single stage, Innovation Action (IA)

Anticipated Project Budget

1000000 €

Coordinator required

No

Duration

156 days

Deadline for EOI

02 Oct 2020

Deadline of the Call

27 Oct 2020

Weblink to the call

https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fec.europa.eu%2Finfo%2Ffunding-tenders%2Fopportunities%2Fportal%2Fscreen%2Fopportunities%2Ftopic-details%2Feic-fti-2018-2020%3BfreeTextSearchKeyword%3D%3BtypeCodes%3D1%3BstatusCodes%3D3109450

Attachments