EINPRESSWIRE

ETSI releases three Reports on Securing Artificial Intelligence for a secure, transparent and explicable AI system

SOPHIA ANTIPOLIS, FRANCE, July 11, 2023 /EINPresswire.com/ -- ETSI is pleased to announce three new Reports developed by its Securing AI group (ISG SAI). They address explicability and transparency of AI processing and provide an AI computing platform security framework. The last Report is a multi-partner Proofs of Concepts framework.

The role of ETSI ISG SAI is to develop guidance to the standards community and its stakeholders so that they have a common understanding of the threats and vulnerabilities of and from AI. The work of the group is therefore informed by, and reactive to, the wider social concerns of AI as well as by the ongoing mission of ETSI to ensure that standards are available to give assurance that security and privacy provisions are available by default to the ICT technologies that our world relies on.

Thus, as stated by Scott Cadzow, the chair of ETSI ISG SAI and ETSI Fellow 2023 "AI is at the same time a threat to how we view ICT and technology as a whole, and an example of the opportunities of those same technologies. The work we are doing in ISG SAI serves our community by protecting against the threats of AI and ensuring that AI systems operate securely, safely and with assurances of privacy across their deployment".

ETSI GR SAI 007 (https://tinyurl.com/3wjrxnxf) on explicability and transparency of AI processing identifies steps to be taken by designers and implementers of AI platforms to give them assurance of the explicability and transparency of AI processing. AI processing includes AI decision making and AI data processing. The Report addresses both static and dynamic forms in order to allow designers to be able to "show their working" (explicability) and to be "open to examination" (transparency). As an example, an AI can be biased by design if the purpose of the AI is to filter candidates for a job based on some personal characteristic (i.e. as opposed to a meritocratic selection engine, the AI acts as a characteristic selection engine). In such a case the explicability and transparency requirements will be able to identify that negative, or trait-based, filtering is at the root of the reasoning engine of the AI.

ETSI GR SAI 009 (https://tinyurl.com/4eehzvm4) provides an Artificial Intelligence computing platform security framework. In an AI system, an AI computing platform acts as the infrastructure for AI applications that provides resource and executing environments. It is therefore essential to study the security of AI computing platforms. The ETSI Report describes a security framework of AI computing platform containing hardware and basic software to protect valuable assets like models and data deployed on AI computing platform when they are used in runtime or stored at rest. The security framework consists of security components in AI computing platform and security mechanisms executed by security components in the platform. By specifying the security framework, an AI computing platform can be consolidated against the relevant attack and can provide security capabilities for stakeholders involved in AI systems who need to better protect the valuable assets (model/data) on an AI computing platform.

ETSI GR SAI 013 (https://tinyurl.com/wmwuk4fu) is a Proof of Concepts framework, providing information about the "lightweight" framework to be used by ETSI ISG SAI to create multi-partner Proofs of Concepts (PoCs). The framework is used as a tool to demonstrate the applicability of ideas and technology. Multi-party PoCs strengthen collaboration between AI stakeholders. The results will put the work of the ETSI SAI group into perspective, will raise visibility and build awareness of the AI security problems. The framework is designed to be inclusive of as many AI-based solutions as possible including those fulfilling critical functions related to data analysis, infrastructures management and (cyber)security. In theory, an AI-based system can become a target on its own, and detection of these types of attacks can pose a significant challenge. However, real-world examples of such attacks are less common. Understanding of the practical aspects to, on one hand conduct an impactful attack against an AI-based system and on the other to defend against and respond to such a threat is still limited and the role of PoCs in highlighting issues is key to the success of the Securing AI.

About ETSI

ETSI provides members with an open and inclusive environment to support the development, ratification, and testing of globally applicable standards for ICT systems and services across all sectors of industry and society. We are a non-profit body, with more than 900 member organizations worldwide, drawn from over 60 countries and five continents. The members comprise a diversified pool of large and small private companies, research entities, academia, government, and public organizations. ETSI is officially recognized by the EU as a European Standardization Organization (ESO). For more information, please visit us at https://www.etsi.org/

Claire Boyer
ETSI
+33 687608440

claire.boyer@etsi.org