The future Internet will rely heavily on virtualization and cloud networking. Therefore, one of the main challenges for the future Internet is to provide such virtual networks and cloud accesses with a high degree of security. This project proposes the design of a framework providing secure identification and authentication, secure data transfer, secure virtualized infrastructure, and privacy in virtual network and clouds, exploring techniques such as microcontrollers, resource management, intrusion tolerant algorithms, and cryptographic protocols. The goal of the SecFuNet project is to design and develop a coherent security architecture for virtual networks and cloud accesses. The proposed architecture will provide solutions allowing the management of the security of communications for all machines connected to a public cloud using virtual networks. Hence, we need a coherent and robust identification scheme as well as a strong authentication system. Algorithms robust to intrusions are also needed for creating a secure environment. Besides, the proposed architecture must guarantee security in the virtualized infrastructure, through isolation of virtual networks and access control for users and managers. The identification of authorized users, however, must not compromise their privacy. Moreover, it is necessary to bring an ergonomic security scheme that is acceptable for all users, even those unknowledgeable in computer science. And finally, the proposed scheme must take into account the heterogeneity of equipment (wireless and wired) to preserve interoperability.

ICT EU-Brazil Coordinated call: