PRISMACLOUD

VISION

PRISMACLOUD is a EU funded research project developing the next generation of cloud security technologies. The project brings novel cryptographic concepts and methods to practical application to improve the security and privacy of cloud based services and make them usable for providers and users.
The main idea and ambition of PRISMACLOUD is to enable end-to-end security for cloud users and provide tools to protect their privacy with the best technical means possible - by cryptography.

METADATA

Call: H2020-ICT-2014-1 • Acronym: PRISMACLOUD • Type of Action: RIA • Partners: 16
Duration: 42 months • Start Date: 2015-02-01 • Estimated Project Cost: ~8.5M Euro
Requested EU Contribution: ~ 8M Euro • Coord.: Austrian Institute of Technology GmbH

OBJECTIVES

1. Development of cryptographic tools to protect the security of data during its lifecycle in the cloud

We aim at the development of cryptographic methods to protect confidentiality, integrity, and authenticity of data at rest beyond standard content encryption and message authentication and, investigation on how authenticity of data can be preserved while processing data and how computing tasks could be outsourced in a verifiable manner.

2. Development of cryptographic tools and methods to protect privacy of users

We aim at the development of cryptographic schemes to preserve privacy of users interacting with cloud services by allowing users to only reveal the information absolutely necessary to make an authorization and to preserve privacy of user related data processed in the cloud guaranteeing that data that is handed to third parties does not leak information about the identities of the data subjects by applying adequate data anonymisation techniques.

3. Creation of enabling technologies for cloud infrastructures

We target the provision of software and hardware implementations of relevant cryptographic mechanisms and development of novel cryptographic techniques to certify the structure of cloud topologies, to prove claims about the certified topology, and to bind topology to component attestation.

4. Development of a methodology for secure service composition

Development of holistic security models and their integration in a seamless way and according to security by design methods. Examination of usability aspects to ensure user acceptance of developments within the project and further research possible monetary benefits based on solid business models and opportunities.

5. Experimental evaluation and validation of project results

The evaluation and validation of the developed methods and tools will be done in three pilots from three different domains, namely healthcare, smart city and e-government. For all stakeholders we will also provision a handbook on secure cloud usage for end users, citizens, policy makers, and security managers.

INNOVATIONS

1. Verifiability of data and infrastructure use

PRISMACLOUD will research and innovate in the field of verifiable computations, functional signatures, as well as in structural integrity for certification of visualized infrastructures. All techniques will help to protect the integrity and authenticity of outsourced data with strong guarantees.

2. User privacy and anonymisation

PRISMACLOUD will innovate, advance and develop cryptographic methods for privacy preserving service usage by means of data minimization and and data anonymisation. These tools are key to seriously consider the cloud environment for hosting services handling sensitive personal data.

3. Securing data at rest

PRISMACLOUD will develop novel techniques to protect the integrity and confidentiality for data stored in the cloud. We will develop methods to store unstructured data which are ideally capable to provide security in the long term and everlasting privacy. Furthermore, different cryptographic tools for structured data and seamless service integration will help to protect data in legacy applications.

4. Secure and efficient implementations

PRISMACLOUD will also deliver efficient and secure implementations complemented with hardware prototyping and security testing for fully integrated solutions. Access to good implementations after the projects are a basic requirement to make the novel technologies available for service integrators.

5. Methodology, tools and guidelines for fast adoption

To facilitate fast adoption of PRISMACLOUD results we further develop holistic security models and methods for secure service composition. Moreover, novel HCI guidelines including HCI design patterns for usable privacy-preserving cryptography and protocols for the cloud will help to design services which respect the users needs and therefore guarantee for best acceptance.

Contact: Thomas Loruenser, AIT Austrian Institute of Technology GmbH, thomas.loruenser@ait.ac.at