TREDISEC: Towards Realizing a Truly Secure and Trustworthy Cloud

by Beatriz Gallego-Nicasio Crespo, Melek Önen and Ghassan Karame

The main goal of the TREDISEC project is to increase trust in cloud technology by providing solutions that enhance data security and provide strong privacy guarantees, without hampering the efficiency-and-reduced-cost attractiveness of existing cloud systems.

The cloud is the go-to technology for companies and businesses these days. Cloud adoption is growing exponentially each year, fueled by new functionalities and capabilities. Although it has many advantages, the cloud also has drawbacks and security-related issues that can make customers shy away from adopting it. Large-scale adoption of the cloud by enterprises and SMEs is hampered by serious concerns about the security and availability of data stored in the cloud. These concerns have been further exacerbated by recent data leak scandals (e.g., corporate data stolen [1], resulting in millions of dollars in losses in just one day) and privacy intrusions (e.g., users' private information illegally accessed and used for blackmail [2]). Moreover, companies are no longer happy to rely on standard cloud security solutions, instead demanding full control over the security and integrity mechanisms employed to protect their data across its lifecycle. As this data is typically a very valuable asset, security and privacy emerge as key features in cloud offerings. TREDISEC addresses these issues by providing a set of security primitives that enhance the resilience of existing cloud infrastructures against attacks and vulnerabilities, protecting data end-to-end, and thus making secure and trustworthy cloud systems a reality.

Achieving end-to-end security within the cloud environment is nevertheless not a straightforward task. Indeed, end-to-end security is at odds with current functionalities offered by the cloud, as shown in Figure 1. For example, while protecting cloud customers' data at rest usually requires data encryption solutions, such a security service inherently refrains cloud services from offering standard APIs for efficiently processing these encrypted data.

TREDISEC addresses security and privacy issues by analyzing, designing and implementing a set of cloud security primitives that are integrated naturally with existing cloud capabilities and functionalities, such as multi-tenancy or storage efficiency. Among other capabilities, these primitives support data reduction, enable secure data processing, enhance data availability and integrity and ensure user isolation and confidentiality in multi-tenant systems. Therefore, the innovation potential of TREDISEC covers:

- Deduplication on encrypted and multi-tenant data
- Means to verify the integrity and availability of multi-tenant data in presence of storage efficiency
- Secure deletion of multi-tenant data in presence of deduplication
- Storage efficiency in presence of securely outsourced database management services
- Secure outsourced analytics/processing in a multi-tenant environment
- Trustworthy, consistent access control for multi-tenancy settings
- Distributed enforcement of access control policies.

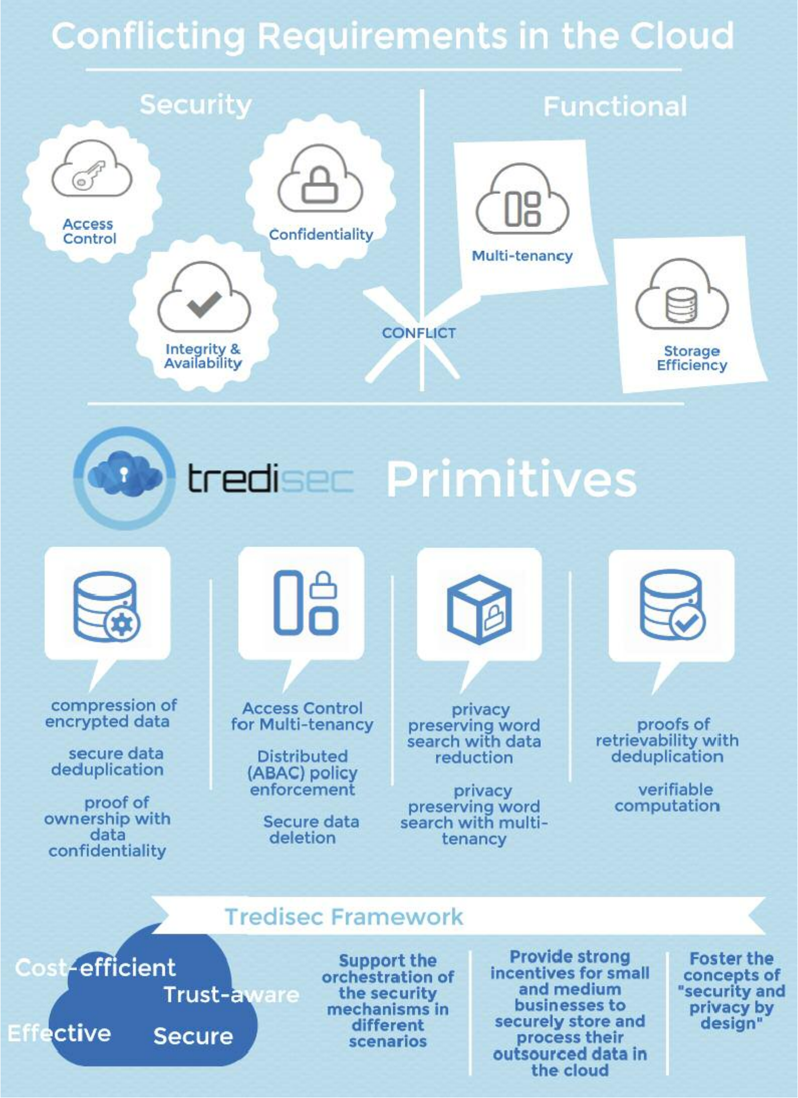
Conflicting Requirements in the Cloud
Security
Functional
Access Control
Confidentiality
Multi-tenancy
Integrity & Availability
CONFLICT
Storage Efficiency
tredisec
Primitives
compression of encrypted data
secure data deduplication
proof of ownership with data confidentiality
Access Control for Multi-tenancy
Distributed (ABAC) policy enforcement
Secure data deletion
privacy preserving word search with data reduction
privacy preserving word search with multi-tenancy
proofs of retrievability with deduplication
verifiable computation
Tredisec Framework
Cost-efficient
Trust-aware
Effective
Secure
Support the orchestration of the security mechanisms in different scenarios
Provide strong incentives for small and medium businesses to securely store and process their outsourced data in the cloud
Foster the concepts of "security and privacy by design"

Figure 1: The TREDISEC approach.

Addressing these innovations is only the first step of the project. The subsequent, and more challenging step, is to consider scenarios with multiple functional and security requirements to evaluate the effectiveness of our approach. These security primitives will be integrated and validated in real use case scenarios designed by four partners of the project, representing diverse business goals (for more detail about use cases see the Links section). Namely, our results will be validated onto (1) the Greek Research and Technology Network's computation and storage cloud (used by the University of Athens), (2) the cloud storage service provided by Arsys, (3) Morpho's identification solutions using biometric data that are stored in the cloud , and finally (4) SAP use case focuses on migration of legacy databases into a secure cloud, which is an important concern for small, midsized and large enterprises that wish to move their day-to-day business processes (e.g., ERP, CRM, HR) to the cloud.

We believe that the results of TREDISEC will have a big impact in business (both large companies and SMEs), allowing them to achieve greater business throughput, and lowering the barriers to enter new markets. We are fully aware of the problem of adoption of new technologies by companies and believe that TREDISEC will cover at least three of the top five barriers: security, data protection, trust, data access, and portability [3].

This paper is a joint work of the TREDISEC project consortium. The TREDISEC project is funded by the H2020 Framework of the European Commission under grant agreement no. 644412. In this project, nine renowned research institutions and industrial players with balanced expertise in all technical aspects of both security and cloud are working together to address the challenges of the project: Atos Spain (project coordinator), NEC Europe, IBM Research, ETH Zurich, Eurecom, Arsys Internet, Greek Research and Technology Network, SAP SE and Morpho (SAFRAN group).

Links:
TREDISEC official website: http://tredisec.eu
TREDISEC Use Cases Definition:
http://tredisec.eu/content/use-cases

References:

[1] Deadline – Sony hack: A Timeline (Last access: 05.11.15), http://kwz.me/QY

[2] Tripwire – The state of security. The Ashley Madison Hack – A Timeline (Last access: 05.11.15), http://kwz.me/QB

[3] European Commission:"Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take", 2012, http://kwz.me/Qr

Please contact:

Beatriz Gallego-Nicasio Crespo
Atos, Spain
Tel: +34 912148800
E-mail: beatriz.gallego-nicasio@atos.net

Smart Devices for the Home of the Future: A New Model for Collaboration

by Daniele Spoladore, Gianfranco Modoni and Marco Sacco

An ontology based approach that aims at enhancing interoperability between home devices and services is being developed by the Italian "Design For All" research project.

Contemporary design is characterized by a major paradigm shift: from traditional design focused on the "average man" to Universal Design, which takes into account a wide variety of possible human needs [1]. This paradigm is also applied to the field of Ambient Assisted Living (AAL) in the design of smart homes, living environments capable of anticipating and responding to the needs of their inhabitants through tailored services provided by diverse devices (e.g. sensors and actuators). However, these smart objects are managed by different software, based on their specific data format. Thus, the home of the future is currently characterized by a wide variety of data, which hinders efficient interactions between the devices involved. In order to address this issue, the Design For All research project, co-funded by the Italian Ministry for Education, University and Research within the cluster of initiatives for Technologies for Ambient Assisted Living, is developing semantic interoperability so that different systems can share and exploit the same information.

The main goal of the project is to develop a software architecture that supports the design phase for future smart homes suitable for any kind of user, enabling distributed devices to adapt to and react with the context. A platform denoted the Virtual Home Framework (VHF) [2] integrates knowledge about the domestic environment, the smart objects and the users. Semantic Web technologies have been adopted to formally describe this information (including the many linking elements) in an ontology, which is a "formal specification of a shared conceptualization" based on first-order logic languages (RDF and OWL). The ontology approach provides a holistic view of the smart home as a whole, considering the physical dimensions, the users involved, and their evolution over the time. It also allows the use of reasoning tools, able to derive new knowledge about the concepts and their relationships, thanks to inferencing rules specified in the Semantic Web Rule Language (SWRL).

The semantic model developed, called the Virtual Home Data Model (VHDM), provides a consistent representation of several knowledge domains; it is composed of several modules including: a) the Physiology model, to keep track of users' medical conditions over time; b) the Smart Object Model, which provides a description of the relationships between appliances and related functionalities; c) the Domestic Environment, which includes information on thermo-hygrometric conditions and air and light quality.