Cloud Security and Privacy by Design

Conference Paper · December 2015

DOI: 10.1007/978-3-319-27164-4_16

3 authors, including:

Thomas Lorünser
AIT Austrian Institute of Technology
51 PUBLICATIONS **629** CITATIONS
SEE PROFILE

Daniel Slamanig
AIT Austrian Institute of Technology
66 PUBLICATIONS **313** CITATIONS
SEE PROFILE

Cloud Security and Privacy by Design

Thomas Lorünser[1], Thomas Länger[2], and Daniel Slamanig[3]

[1] AIT Austrian Institute of Technology, Austria
thomas.loruenser@ait.ac.at
[2] University of Lausanne, Switzerland
thomas.laenger@unil.ch
[3] Graz University of Technology, Austria
daniel.slamanig@iaik.tugraz.at

Abstract. In current cloud paradigms and models, security and privacy are typically treated as add-ons and are not adequately integrated as functions of the cloud systems. The EU Project PRISMACLOUD (Horizon 2020 programme; duration 2/2015-7/2018) sets out to address this challenge and yields a portfolio of novel technologies to build security enabled cloud services, guaranteeing the required security by built-in strong cryptography.

Keywords: Secure cloud computing, cryptography, privacy, information theoretic security, usability, security by design

1 Motivation and Objectives

With an annual turnover in the region of USD 150 billion, and with huge growing rates, the market for cloud computing can be considered as a major growth area in ICT [14]. Several technology research and advisory firms attribute a bright economic future, e.g., the management consulter Accenture states that 46% of all IT spending by 2016 will be for cloud-related platforms and applications [10]. The European Commission promotes in its "European Cloud Computing Strategy" of 2012 [4] the rapid adoption of cloud computing in all sectors of the economy to boost productivity. The Commission concludes that "cloud computing has the potential to slash users' IT expenditure and to enable many new services to be developed. Using the cloud, even the smallest firms shall be able to reach out to ever larger markets, while it will enable governments to make their services more attractive and efficient while at the same time cueven while reining in spending."

Cloud computing is a new delivery model of processing, storage and communication resources and will be at the heart of future ICT applications. In combination with other IT mega-trends like Big Data and the Internet of Things, it will give rise to many new smart applications in numerous domains. However, besides the benefits of cloud computing, new problems are arising. Many are not yet sufficiently solved, especially information security and privacy problems. The fundamental concept of the cloud is storage and processing by a third party (the cloud service provider) which is no longer comparable to traditional outsourcing, especially when a public cloud service is used. The intrinsic multi-tenancy

of cloud computing and the broad connectivity introduces new security threats, leading to tremendous risk for personal and sensitive data. Organizational and legal tools have been introduced to increase trust in the cloud provider, but recent incidents show that these measures are by far not sufficient to guard personal data and trade secrets against illegal interceptions, insider threats, or vulnerabilities.

The PRISMACLOUD consortium aims at a new approach towards cloud security within the EU Horizon 2020 research framework. For us, the only reasonable way to achieve the required security properties for outsourced data is by adopting suitable cryptographic mechanisms. Thus, the goal of PRISMACLOUD is to develop the next-generation of cryptographically secured cloud services with security and privacy built in by design and from end-to-end. The main objectives of PRISMACLOUD are:

- Development of cryptographic tools to protect the security of data during its lifecycle in the cloud
- Development of cryptographic tools and methods to protect privacy of users
- Creation of enabling technologies for cloud infrastructures
- Development of a methodology for secure service composition
- Experimental evaluation and validation of project results

The outcome of the project will contribute to enable trustworthy and privacy preserving services to be deployed in only partially trusted cloud infrastructures, i.e. in the public cloud setting.

2 Concept and Approach

The concept underlying PRISMACLOUD is to develop and improve novel cryptographic technologies and to study how they can be integrated in a user-friendly way for improving the security of services for both businesses and individuals. Ideally data in the cloud shall be protected from end-to-end with strong cryptographic guarantees and users shall remain in full control over their data. At the same time, privacy enhancing technologies shall be applied to minimize the information a client involuntarily discloses while using a cloud service. The project will present new secure cloud technologies for European citizens, administration, and industries, with strong security guarantees capable of increasing trust in outsourcing storage and computation to the cloud.

The PRISMACLOUD approach is centred around research and development activities for bringing recent and novel cryptographic tools to practical application. Innovations for trustworthy cloud computing shall be created to the benefit of European industry and society [4]. The main pillars in PRISMACLOUD enable *verifiability of the cloud*, improve *privacy enhancing technologies* and develop methods for protecting *confidentiality and integrity for data at rest*. Furthermore, a broad set of accompanying measures will be carried out for assisting the introduction of the new technologies to the market and thus to the user.

To enable **verifiability**, we develop *verifiable and authenticity preserving data processing tools*. The correctness of outsourced computations (e.g., by means of [15, 2]) will be verified, and malleable as well as functional signatures (cf. [3]) will secure the authenticity and verifiability of processes and workflows. These cryptographic primitives allow for controlled modification of authenticated data. Every modification beyond what is allowed renders the authentication tag (i.e,. signature or tag of a message authentication code) invalid. Although currently only linear functions (like counting and summation) and polynomial functions of bounded degree (like variance) are practically usable from a performance point of view, we have identified applications, e.g. in our eHealth pilot, where such tools allow to greatly improve the security of services, i.e., the leakage of sensitive data can be effectively reduced when processing data in the cloud.

Another technology in the field of verifiability provides means to digitally sign graph representations of virtualised infrastructures [6]. Basically, such a signature binds the verification of a (human) cloud auditor to an actual infrastructure and it enables the infrastructure provider to prove topology properties of the virtualised infrastructure (like connectivity isolation) to customers without revealing too much details of the topology (e.g., information about configurations of other tenants also using the infrastructure). In PRISMACLOUD we will develop the necessary tools to verify and certify the *integrity of virtualized infrastructures*.

Research in data minimization technologies for *privacy preserving service usage* will increase the **privacy of users**. It is usually not necessary for users to reveal more than very little information when needing to prove an authorisation or the possession of a right. Still, the cloud provider must be cryptographically reassured of the user's authorization. We will use technology related to *attribute-based anonymous credentials* (Privacy ABCs) [1] and related concepts to enable the implementation of privacy protecting and data minimising authentication and authorisation systems for cloud applications and services. Such primitives allow to encode attributes into digital credentials in a way, that attributes can be selectively disclosed (or statements about the encoded attributes can be proven without revealing their effective values) in an anonymous and unlinkable way. Privacy ABCs will enable users to prove to services that they are authorized while respecting data minimization and without having to reveal their identity.

We will also improve methods for the *anonymization of big data* and demonstrate its' applicability in the healthcare domain, i.e. for the purpose of medical research. Thereby, algorithmic approaches such as *k-anonymity* [13] provide a tool for preventing subjects of the data to be identified, while leaving the data practically useful for analysis. As, however, achieving optimal k-anonymity is **NP**-hard [8], these approaches are currently only suitable for relatively small data set. Our goal is to improve the effectively of these approaches for the anonymization of very large data sets.

For **protecting data at rest**, we support novel concepts, which will at the same time enable dynamic collaboration, as well controlled sharing of information. Currently, most available cloud storage services store the data either

unencrypted or apply encryption which remains under complete control of the cloud service provider; some cloud users wrap a layer of cryptography around their data before they store it in the cloud. In the first case, the cloud provider has to be trusted to provide effective protection of the data as regards confidentiality and integrity. This includes all copies and replications of the data which are created for availability purposes in all layers of the storage architecture. Users also have to consider, that the cloud provider is capable of reading all the data in plain and has to be trusted not to exploit that knowledge. In the second case, collaboration on the data is severely impeded, and availability of the data is threatened if the user loses its cryptographic keys.

For *unstructured data*, we will develop a new distributed system approach by applying the cloud-of-clouds paradigm. The cryptographic storage network for the secure, distributed storage of data uses an information-dispersal algorithm, based on secret sharing mechanisms [11]. The information is split into a number of shares, of which any subset of a fixed number allows the reconstruction of the original data. This approach is capable of *long-term security and everlasting privacy* [9]. We will investigate methods to efficiently realize such systems with improved practical usability [12, 7]. In the case of structured data or legacy applications, we will supply *cryptography for seamless service integration*, and in particular format- as well as order-preserving encryption and tokenization [17].

The cryptography research and implementation in PRISMACLOUD is accompanied by **methodology, guidelines, and evaluation** activities, supporting the diffusion of the results to the users. A *standards action plan* containing a set of recommendations and recommended actions to ensure an optimized impact of PRISMACLOUD results for qualified practical application will be developed in accordance with the European Cloud Computing Strategy's goals to "help cloud take off" [4]. We will present a *holistic security model* and methods to compose security and privacy preserving services in a convenient way. *Usability concepts and end-user aspects* are taken seriously and will guide all technical aspects in the project [16]. Besides licit use, we will assess the impact of potential criminal uses and misuses of the secure cloud infrastructures to foster, enhance, and promote cybercrime [5].

The PRISMACLOUD results shall be practically *demonstrated and validated* by demonstrating implementations of three industry contributed use cases in the domains of eHealth, eGovernment, and smart city, where personal and other data of highest sensitivity is involved.

References

1. Camenisch, J., Lehmann, A., Neven, G.: Electronic Identities Need Private Credentials. IEEE Security & Privacy 10(1), 80–83 (2012), `http://doi.ieeecomputersociety.org/10.1109/MSP.2012.7`
2. Catalano, D.: Homomorphic Signatures and Message Authentication Codes. In: SCN. LNCS, vol. 8642, pp. 514–519. Springer (2014)

3. Demirel, D., Derler, D., Hanser, C., Pöhls, H.C., Slamanig, D., Traverso, G.: PRISMACLOUD D4.4: Overview of Functional and Malleable Signature Schemes. Tech. rep., H2020 Prismacloud, www.prismacloud.eu (2015)
4. European Commission: European cloud computing strategy "unleashing the potential of cloud computing in europe" (2012), http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy, (online 31.3.2015)
5. Ghernaouti, S.: Cyber Power - Crime, Conflict and Security in Cyberspace. EPFL Press (2013)
6. Groß, T.: Signatures and Efficient Proofs on Committed Graphs and NP-Statements. In: Financial Cryptography. LNCS, Springer (2015)
7. Lorünser, T., Happe, A., Slamanig, D.: ARCHISTAR: Towards Secure and Robust Cloud Based Data Sharing. In: IEEE 7th International Conference on Cloud Computing Technology and Science, CloudCom 2015, Vancouver, November 30 - December 3. IEEE (2015)
8. Meyerson, A., Williams, R.: On the complexity of optimal k-anonymity. Symposium on Principles of Database Systems, PODS '04, New York, U.S.A. (2004)
9. Müller-Quade, J., Unruh, D.: Long-Term Security and Universal Composability. J. Cryptology 23(4), 594–671 (2010)
10. PRWeb: A cloud computing forecast summary for 2013-2017 from idc, gartner and kpmg, citing a study by accenture (2013), http://www.prweb.com/releases/2013/11/prweb11341594.htm, (online 31.3.2015)
11. Shamir, A.: How to share a secret. Commun. ACM 22(11), 612–613 (1979)
12. Slamanig, D., Hanser, C.: On Cloud Storage and the Cloud of Clouds Approach. In: ICITST-2012. pp. 649–655. IEEE Press (2012)
13. Sweeney, L.: k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems (10 (5)), 557–570 (2002)
14. Transparency Market Research: Cloud computing services market – global industry size, share, trends, analysis and forecasts 2012-2018 (2012), http://www.transparencymarketresearch.com/cloud-computing-services-market.html, (online 31.3.2015)
15. Walfish, M., Blumberg, A.J.: Verifying Computations without Reexecuting Them. Commun. ACM 58(2), 74–84 (2015)
16. Wästlund, E., Angulo, J., Fischer-Hübner, S.: Evoking comprehensive mental models of anonymous credentials. In: iNetSeC. pp. 1–14 (2011)
17. Weiss, M., Rozenberg, B., Barham, M.: Practical solutions for format-preserving encryption. CoRR abs/1506.04113 (2015), http://arxiv.org/abs/1506.04113