

Towards a New Paradigm for Privacy and Security in Cloud Services

Thomas Lorüenser^{1(✉)}, Charles Bastos Rodriguez², Denise Demirel³,
Simone Fischer-Hübner⁴, Thomas Groß⁵, Thomas Länger⁶, Mathieu des Noes⁷,
Henrich C. Pöhls⁸, Boris Rozenberg⁹, and Daniel Slamanig¹⁰

¹ AIT Austrian Institute of Technology, Vienna, Austria
`thomas.loruenser@ait.ac.at`

² ATOS Spain S.A., Madrid, Spain

³ Technische Universität Darmstadt, Darmstadt, Germany

⁴ Karlstad University, Karlstad, Sweden

⁵ Newcastle University, Newcastle upon Tyne, UK

⁶ University of Lausanne, Lausanne, Switzerland

⁷ Commissariat à l'énergie atomique et aux énergies alternatives, Grenoble, France

⁸ University of Passau, Passau, Germany

⁹ IBM Haifa Research Lab, Haifa, Israel

¹⁰ Graz University of Technology, Graz, Austria

Abstract. The market for cloud computing can be considered as the major growth area in ICT. However, big companies and public authorities are reluctant to entrust their most sensitive data to external parties for storage and processing. The reason for their hesitation is clear: There exist no satisfactory approaches to adequately protect the data during its lifetime in the cloud. The EU Project PRISMACLOUD (Horizon 2020 programme; duration 2/2015–7/2018) addresses these challenges and yields a portfolio of novel technologies to build security enabled cloud services, guaranteeing the required security with the strongest notion possible, namely by means of cryptography. We present a new approach towards a next generation of security and privacy enabled services to be deployed in only partially trusted cloud infrastructures.

1 A New Take on Cloud Security

1.1 Introduction

Today, cloud computing is already omnipresent and starts pervading all aspects of our life, whether in the private area or in the business domain. The annual market value related to cloud computing is estimated to be in the region of USD 150 billion, and will probably grow by the year 2018 to around USD 200 billion [36, 41]. The European Commission (EC) promotes in its strategy Digital Agenda for Europe/Europe 2020 the rapid adoption of cloud computing in all sectors of the economy to boost productivity. Furthermore, the EC 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 can reach out to ever larger markets while governments can make their services more attractive and efficient even while reining in spending. [20].

However, besides these advantages of cloud computing, many new problems arise which are not yet sufficiently solved, especially with respect to information security and privacy [16, 21, 32]. The fundamental concept of the cloud is storage and processing by a third party (the cloud or service provider), which actually invalidates the traditional view of a perimeter in IT security. In fact, the third party becomes part of the company's own computation and storage IT infrastructure albeit not being under its full control. This situation is very problematic. Thus, economic incentives and legal tools such as service level agreements (SLAs) have been introduced to increase trust in the service provider. However, 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 exposing data to unauthorized parties. While being processed by a provider, data is typically neither adequately protected against unauthorized read access, nor against unwanted modification, or loss of authenticity. Consequently, in the most prominent cloud deployment model today – the public cloud – the cloud service provider necessarily needs to be trusted. Security guarantees with respect to user data can only be given on a contractual basis and rest to a considerable extent on organisational (besides technical) precautions. Hence, outsourcing IT tasks to an external shared infrastructure builds upon a problematic trust model. This situation inhibits many companies in the high-assurance and high-security area to benefit from external cloud offerings: for them confidentiality, integrity, and availability are of such major importance that adequate technical measures are required—but state-of-the-art ICT can currently not provide them. Moreover, individuals using public cloud services face a considerable privacy threat too, since they typically expose more information than required to services.

1.2 Objectives

In this work we present a new approach towards cloud security which is developed by the PRISMACLOUD consortium within the EU Horizon 2020 research framework. For us, the only reasonable way to achieve the required security properties for outsourced data storage and processing is by adopting suitable cryptographic mechanisms. Thus, the vision of PRISMACLOUD is to develop the next-generation of cryptographically secured cloud services with security and privacy built in by design.

The main objectives of PRISMACLOUD are: (i) to develop next-generation cryptographically secured services for the cloud. This includes the development of novel cryptographic tools, mechanisms, and techniques ready to be used in a cloud environment to protect the security of data over its lifecycle and to protect the privacy of the users. The security shall be based on by design principles. (ii) to assess and validate the project results by fully developing and implementing three realistic use case scenarios in the areas of e-government, healthcare, and smart city services. (iii) to conduct a thorough analysis of the security of the final systems, their usability, as well as legal and information governance aspects of the new services.

The European Commission already recognised the potential future impact of cloud computing for all of us and has issued a cloud computing strategy [20]. The aim of this strategy is to protect European citizens from potential threats, while simultaneously unleashing the potential of cloud computing, for both the industry/public sector as well as for individuals. PRISMACLOUD is backing this strategy and will help to remove a major inhibitor against cloud adoption in security relevant domains by developing cloud applications, that preserve more security and privacy for citizens. It will further help to strengthen the position of European industries in the cloud domain and also strengthen European research in a field with high research competition.

1.3 EU Research Context

Ongoing research activities like SECCRIT, Cumulus, and PASSIVE¹ are extremely valuable and will be setting the standards and guidelines for secure cloud computing in the next years. However, these approaches consider the cloud infrastructure provider as being trustworthy in the sense that no information of the customers, i.e., tenants, will be leaked, nor their data will be tampered with. The cloud infrastructure provider, however, has unrestricted access to all physical and virtual resources and thus absolute control over all tenants' data and resources. The underlying assumption is, that if the cloud provider performs malicious actions against its customers, in the long run, he or she will be put out of business – if such doings are revealed. However, this assumption is very strong, especially considering the ongoing revelation of intelligence agencies' data gathering activities. Data disclosure may even be legally enforced in a way completely undetectable by the cloud provider's customers.

Through auditing and monitoring of cloud services, some of the malicious behaviour of outsiders and insiders (e.g., disgruntled employees with administrator privileges) may be detectable *ex-post*. However, that does not help a specific victim to prevent or survive such an attack. Moreover, advanced cyber-attacks directly targeting a specific victim can barely be detected and prevented with cloud auditing mechanisms or anomaly detection solutions. These methods are more efficient for the detection of large scale threats and problems and for making the infrastructure itself resilient, while keeping an acceptable level of service.

Other projects, like TClouds and PRACTICE² take cloud security a step further: TClouds already considers the impact of malicious provider behaviour and tries to protect users. However, it is not strongly focusing on comprehensive integration of cryptography up to the level of end-to-end security. PRACTICE, in contrast, is well aligned with our idea of secure services by means of cryptography. However, it focuses mainly on the preservation of data confidentiality for processing, when outsourced to the cloud. PRISMACLOUD is complimentary to these concepts and enhance them with cryptographic primitives for the verification of outsourced computation and other relevant functionalities to be carried

¹ EU-FP7: <http://www.seccrit.eu/>, <http://www.cumulus-project.eu/>, <http://ict-passive.eu/>.

² EU-FP7: <http://www.tclouds-project.eu>, <http://www.practice-project.eu/>.

out on the data in the untrusted cloud. Research activities in context of privacy in cloud computing were and are currently conducted by various projects like ABC4Trust, A4Cloud, and AU2EU³. PRISMACLOUD complements these efforts by further developing privacy-enhancing technologies for the use in cloud based environments.

1.4 Main Innovations

The main goal of PRISMACLOUD is to enable the deployment of highly critical data to the cloud. The required security levels for such a move shall be achieved by means of novel security enabled cloud services, pushing the boundary of cryptographic data protection in the cloud further ahead. PRISMACLOUD core innovations are presented in the following sections.

In Sect. 2.1 we outline the idea of outsourcing computations with verifiable correctness and authenticity-preservation as well as cryptographic techniques for the verification of claims about secure configurations of the virtualized cloud infrastructures. In Sect. 2.2 we discuss cryptographic data minimization and anonymization technologies. Section 2.3 outlines a distributed multi-cloud data storage architecture which shares data among several cloud providers and thus improves data security and availability. Such techniques shall avoid vendor lock-in and promote a dynamic cloud provider market, while preserving data authenticity and facilitating long-term data privacy. Additionally, we discuss cryptographic tools for a seamless integration of encryption into existing cloud services. The PRISMACLOUD work program is complemented with activities described in Sect. 3 addressing secure service composition, usability, and secure implementation and evaluation of results in pilots. In order to converge with the European Cloud Computing Strategy, a strategy for the dissemination of results into standards will also be developed within PRISMACLOUD.

2 Technical Innovations

In this section we briefly outline technical tools and concepts which summarize the technical innovations within PRISMACLOUD.

2.1 Verifiability of Data, Processing, and Infrastructure

Verifiable and Authenticity Preserving Data Processing. Verifiable computing aims at outsourcing computations to one or more untrusted processing units in a way that the result of a computation can be efficiently checked for validity. General purpose constructions for verifiable computations have made significant process over the last years [42]. There are already various implemented systems which can be deemed nearly practical, but are not yet ready for real-world

³ EU-FP7: <https://abc4trust.eu>, <http://www.a4cloud.eu>, <http://www.au2eu.eu>.

deployment. Besides general purpose systems, there are other approaches that are optimized for specific (limited) classes of computations or particular settings, e.g., [2, 14, 22].

In addition to verifiability of computations, another interesting aspect is to preserve the authenticity of data that is manipulated by computations. Tools for preserving authenticity under admissible modifications are (fully) homomorphic signatures (or message authentication codes) [13]. Besides this general tool, there are signatures with more restricted capabilities, like redactable signatures introduced in [29, 40], which have recently shown to offer interesting applications [26, 35]. These and other functional and malleable signatures will be developed further within PRISMACLOUD to meet requirements set by cloud applications. By combining these cryptographic concepts, PRISMACLOUD aims at providing tools that allow to realize processes (with potentially various participating entities) that guarantee to preserve the authenticity and provide verifiability of involved data and computations respectively.

Integrity and Certification of Virtualized Infrastructure. The area of structural integrity and certification of virtualized infrastructures bridges between three areas: 1. attestation of component integrity, 2. security assurance of cloud topologies, and 3. graph signatures to connect these areas.

Attestation is the process in which a trusted component asserts the state of a physical or virtual component of the virtualized infrastructure, on all the layers of it. PRISMACLOUD builds upon Direct Anonymous Attestation (DAA) [9] as means to enable this assertion while preserving confidentiality and privacy. Cloud security assurance offers the analysis of cloud topologies for security properties [6–8] as well as the verifiable auditing that these properties are maintained [37]. Graph signatures [24], that is, signatures on committed graphs, are a new primitive we investigate within PRISMACLOUD, which allow two parties to engage in an interactive protocol to issue a signature on a graph. The resulting signature allows to convince a verifier that the signed graph fulfils certain security properties (e.g., isolation or connectedness) without disclosing the blueprint of the graph itself. Within PRISMACLOUD we develop and optimize the use of graph signatures for practical use in virtualized infrastructures. Their application allows an auditor to analyse the configuration of a cloud, and to issue a signature on its topology (or a sequence of signatures on dynamically changing topologies). The signature encodes the topology as a graph in a special way, such that the cloud provider can prove high-level security properties such as isolation of tenants to verifiers. Furthermore, we will bridge between cloud security assurance and verification methodology and certification. We do this by establishing a framework that issues signatures and proves security properties based on standard graph models of cloud topologies and security goals stated in formal language, such that the virtualization assurance language VALID [5].

2.2 User Privacy Protection and Usability

Privacy Preserving Service Usage. For many services in the cloud it is important that users are given means to prove their authorisation to perform

or delegate a certain task. However, it is not always necessary that users reveal their full identity to the cloud, but only prove by some means that they are authorised, e.g., possess certain rights. The main obstacle in this context is that a cloud provider must still be cryptographically reassured that the user is authorised.

Attribute-based anonymous credential (ABC) systems have proven to be an important concept for privacy-preserving applications. They allow users to authenticate in an anonymous way without revealing more information than absolutely necessary to be authenticated at a service. Thus, there are strong efforts to bring them to practice⁴. Well known ABC systems are, for instance, the multi-show system Idemix [11] and the one-show system U-Prove [33]. Recently also some alternative approaches for ABC systems from malleable signature schemes [12, 15] and a variant of structure-preserving signatures [27] have been proposed.

In PRISMACLOUD we aim at improving the state of the art in ABC systems and related concepts with a focus on their application in cloud computing services. Besides traditional applications such as for anonymous authentication and authorization we will also investigate their application to privacy-preserving billing [17, 38] for cloud storage and computing services.

Big Data Anonymization. Anonymizing data sets is a problem which is often encountered when providing data for processing in cloud applications in a way, that a certain degree of privacy is guaranteed. However, achieving optimal k -anonymity, for instance, is known to be an NP-hard problem. Typically, researchers have focused on achieving k -anonymity with minimum data loss, thus maximizing the utility of the anonymised results. But all of these techniques assume that the dataset to be anonymised is relatively small (and fits into computer memory). In the last few years several attempts have been made to tackle the problem of anonymising large datasets.

In PRISMACLOUD, we aim to improve existing anonymisation techniques in terms of both performance and utility (minimizing information loss) for very large data sets. We strive to overcome deficiencies in current mechanisms, e.g., size limitations, speed, assumptions about quasi-identifiers, or existence of total ordering, and implement a solution suitable for very large data sets. In addition, we address issues related to distribution of very large data sets.

2.3 Securing Data (at Rest)

Confidentiality and Integrity for Unstructured Data. Protecting customer data managed in the cloud from unauthorised access by the cloud provider itself should be one of the most basic and essential functionalities of a cloud system. However, the vast majority of current cloud offerings does not provide such a functionality. One reason for this situation is that current cryptographic solutions can not be easily integrated without drastically limiting the capabilities of the storage service.

⁴ e.g., ABC4Trust: <https://abc4trust.eu/>.

In PRISMACLOUD, we aim to research and develop novel secure storage solutions which are based on secret sharing and have increased flexibility. Secret sharing can also be used to provide confidentiality and integrity for data at rest with strong security guarantees in a key-less manner when working in a distributed setting. Various systems have been proposed during the last years, but most of them work in rather naive single user modes and require a trusted proxy in their setting [39]. In [4] a new type is proposed, which uses semi-active nodes to support concurrency in data storage access. It combines efficient Byzantine protocols with various types of secret sharing protocols to cope with different adversary settings in a flexible way. However, desired features such as multi-user support through the integration of a trustworthy distributed access control system or mechanisms for access privacy are still missing.

Our goal is to develop efficient and flexible secret sharing based storage solutions for dynamic environments, like the cloud, supporting different adversary models (active, passive, mixed) and multiple users. The research will focus on the design of a fully decentralized system without single-point-of-trust and single-point-of-failure. Moreover, we will also investigate how metadata can be protected to have better access privacy.

Long-Term Security Aspects and Everlasting Privacy. To provide protection goals, such as integrity, authenticity, and confidentiality in the long-term, classic cryptographic primitives like digital signatures and encryption schemes are not sufficient. They become insecure when their security properties are defeated by advances in computer power or cryptanalytic techniques. Thus, the only approach known to address long-term confidentiality is by using proactive secret sharing, e.g., [25]. In this approach, the data is split into several shares that are stored in different locations and are renewed from time to time. Although secret sharing is needed to provide long-term confidentiality, there is no approach that allows performing publicly or privately verifiable computations or integrity preserving modifications on secret shares yet. Besides the distributed storage of data, to provide everlasting privacy (or confidentiality) for data processed in a publicly verifiable manner, the information published for auditing needs to be information-theoretically secure. Only a few solutions address this and only for specific problems, such as verifiable anonymisation of data [10] and verifiable tallying of votes, e.g., [30]. No general applicable solution is provided, nor do existing approaches show how authenticated data can be processed in a publicly verifiable way. Therefore, we aim at providing solutions for proactive secret sharing of authenticated data and techniques that allow for privately and publicly verifiable computations.

Cryptography for Seamless Service Integration. For existing applications in the cloud, it may be impossible to transparently add security features later on. Assume, for instance, encrypted data is stored in the same database table used for unencrypted data. In this case applications running on the database may be unable to use the encrypted data, causing them to crash or alternatively,

to output incorrect values. Standard encryption schemes are designed for bit-strings of a fixed length and can therefore significantly alter the data format, which may cause disruptions both in storing and using the data.

To address this problem, techniques like format-preserving encryption (FPE), order-preserving encryption (OPE), and tokenization have emerged as most useful tools. In FPE schemes the encrypted ciphertexts have the same format as the messages, i.e. they can be directly applied without adapting the application itself. OPE schemes, on the other hand, maintain the order between messages in the original domain, thus allowing execution of range queries on encrypted data.

In PRISMACLOUD we aim to address the shortcomings of the existing FPE and OPE schemes. It can be shown that existing FPE schemes for general formats, e.g., name, address, etc., are inefficient, lack in their security level, and do not provide a clear way for format definition, thus making them practically unusable. We propose to address both issues (security and efficiency) and develop an FPE scheme for general formats that: *(i)* is more efficient; *(ii)* provides an acceptable security guarantee; *(iii)* supports a complex format definition; *(iv)* could be employed to solve practical problems, e.g., data sharing for clusters of private clouds. For OPE we aim to further progress the state of the art from both security and performance perspectives.

3 Methodology, Guidelines, and Evaluation

In this section we discuss how our technical innovations will be put to practice and how user's trust in these solutions will be improved.

3.1 Holistic Security Models

We have previously described many cryptographically strong building blocks. However, combining the building blocks of PRISMACLOUD correctly would require the developers to have a solid understanding of their cryptographic strength. The approach of service orientation [19] has increasingly been adopted as one of the main paradigms for developing complex distributed systems out of re-usable components called services. PRISMACLOUD aims to use the potential benefits of this software engineering approach, but not build yet another semi-automated or automated technique for service composition. To compose these building blocks into secure higher level services without an in-depth understanding of their cryptographic underpinnings PRISMACLOUD will identify which existing models for the security of compositions are adequate to deal with the complexity and heterogeneity.

PRISMACLOUD will adopt working and established solutions and assumes that the working way of composing services can be a way to allow secure composition. When each service can be described using standard description languages this allows extending composition languages [3] to provide further capabilities, e.g., orchestrations, security, and transactions, to service-oriented solutions [34]. In PRISMACLOUD we want to reduce the complexity further, just like recently,

mashups [18] of web APIs provided means for non-experts to define simple workflows. Within PRISMACLOUD we will develop a description of not only the functionality of each cryptographic building block but also of their limitations and composability.

3.2 Usability Concepts and End-User Aspects

Cryptographic tools, such as secret sharing, verifiable computation, or anonymous credentials, are fundamental technologies for secure cloud services and to preserve end users' privacy by enforcing data minimization. End users are still unfamiliar with such cryptographic concepts that are counterintuitive to them and for which no obvious real-world analogies exist. In previous HCI studies it has been shown that users have therefore difficulties to develop the correct mental models for data minimisation techniques such as anonymous credentials [43] or the new German identity card [28]. Moreover, end users often do not trust the claim that such privacy-enhancing technologies will really protect their privacy [1]. Similarly, users may not trust claims of authenticity and verifiability functionality of malleable and of functional signature schemes. In our earlier research work, we have explored different ways in which comprehensive mental models of the data minimization property of anonymous credentials can be evoked on end users [43]. PRISMACLOUD extends this work by conducting research on suitable metaphors for evoking correct mental models for other privacy-enhancing protocols and cryptographic schemes used in PRISMACLOUD. Besides, it researches what social trust factors can establish trust in PRISMACLOUD technology and how this can be matched into the user interfaces.

Moreover, previous studies have shown the vulnerability of information and communication technology systems, and especially also of cloud systems, to illegal and criminal activities [23]. We will take a critical appraisal of the secure cloud systems proposed in PRISMACLOUD and will analyze, whether they live up to the security promises in practical applications. We will give an indication for individuals, and for corporate and institutional security managers, what it means in practice to entrust sensitive data in specific use cases to systems claiming to implement, e.g., “everlasting privacy” [31]. 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. We want to anticipate threats resulting from misuse, deception, hijacking, or misappropriation by licit entities.

3.3 Demonstration and Evaluation

As feasibility proof, three use cases from the fields of smart city, E-Government, and E-Health will be augmented with the PRISMACLOUD tools in accordance with the elaborated methodologies and evaluated by the project participants.

In the *Smart City* domain, the privacy tools will be used to augment a prototype of the European disabled batch implementation⁵ with data minimization technologies. Furthermore, an end-to-end secure information sharing system will

⁵ EU-FP7 SIMON Project: <http://www.simon-project.eu>.

help to protect confidentiality, integrity, and availability of surveillance data of public areas for law enforcement units. In the *E-Government* domain, we will develop a secure community cloud approach, where governmental IT service providers are able to pool their resources for increased availability and business continuity. In a semi-trusted model every provider shares parts of its storage infrastructure with other providers in a verifiable manner but without breaking confidentiality of data. In addition, it hosts some business support services in an authentic way. The protection of integrity and authenticity of health data will be demonstrated in the *E-Health* scenario, where telemedicine data will be secured throughout their whole life-cycle in the cloud with increased agility. The data will be even processed in a verifiable manner to avoid tampering of third parties with sensitive personal information.

4 Conclusion and Outlook

According to the importance of the project goals, i.e. to enable secure dependable cloud solutions, PRISMACLOUD will have a significant impact in many areas. On a European level, PRISMACLOUD's disruptive potential of results lies in its provision of a basis for the actual implementation and deployment of security enabled cloud services. Jointly developed by European scientists and industrial experts, the technology can act as an enabling technology in many sectors, like health care, electronic government, and smart cities. Increasing adoption of cloud services, with all its positive impact on productivity, and creation of jobs may be stimulated. On a societal level, PRISMACLOUD potentially removes a major roadblock towards the adoption of efficient cloud solutions to a potential benefit of the end-users. Through the use of privacy-preserving data minimization functionalities, and depersonalization features, the amount of data being collected about end-users may effectively be reduced, maintaining the full functionality of the services. We will explicitly analyse potential negative consequences and potential misuses (cybercrime) of secure cloud services. Additionally, the potential impact for European industry is huge: PRISMACLOUD results may contribute to pull some of the cloud business currently concentrated elsewhere to Europe and create sustainable business opportunities for companies in Europe. Equally important is the potential impact of PRISMACLOUD for the European scientific community, as its results will be very much on the edge of scientific research.

Acknowledgements. This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644962.

References

1. Andersson, C., Camenisch, J., Crane, S., Fischer-Hübner, S., Leenes, R., Pearson, S., Pettersson, J.S., Sommer, D.: Trust in PRIME. In: ISSPIT, pp. 552–559 (2005)
2. Backes, M., Fiore, D., Reischuk, R.M.: Verifiable delegation of computation on outsourced data. In: ACM CCS, pp. 863–874. ACM (2013)

3. Beek, M.T., Bucchiarone, A., Gnesi, S.: A Survey on Service Composition Approaches: From Industrial Standards to Formal Methods. Technical report 2006-TR-15 (2006)
4. Bessani, A., Correia, M., Quaresma, B., André, F., Sousa, P.: Depsky: dependable and secure storage in a cloud-of-clouds. *Trans. Storage* **9**(4), 1–12 (2013)
5. Bleikertz, S., Groß, T.: A virtualization assurance language for isolation and deployment. In: *POLICY*. IEEE, June 2011
6. Bleikertz, S., Groß, T., Mödersheim, S.: Security analysis of dynamic infrastructure clouds (extended abstract), September 2013
7. Bleikertz, S., Groß, T., Schunter, M., Eriksson, K.: Automated information flow analysis of virtualized infrastructures. In: Atluri, V., Diaz, C. (eds.) *ESORICS 2011*. LNCS, vol. 6879, pp. 392–415. Springer, Heidelberg (2011)
8. Bleikertz, S., Vogel, C., Groß, T.: Cloud radar: near real-time detection of security failures in dynamic virtualized infrastructures. In: *ACSAC*, pp. 26–35. ACM (2014)
9. Brickell, E., Camenisch, J., Chen, L.: Direct anonymous attestation. In: *ACM CCS*, pp. 225–234. ACM Press (2004)
10. Buchmann, J., Demirel, D., van de Graaf, J.: Towards a publicly-verifiable mix-net providing everlasting privacy. In: *Financial Cryptography*, pp. 197–204 (2013)
11. Camenisch, J., Herreweghen, E.V.: Design and implementation of the idemix anonymous credential system. In: *ACM CCS*, pp. 21–30. ACM (2002)
12. Canard, S., Lescuyer, R.: Protecting privacy by sanitizing personal data: a new approach to anonymous credentials. In: *ASIA CCS*, pp. 381–392. ACM (2013)
13. Catalano, D.: Homomorphic signatures and message authentication codes. In: Abdalla, M., De Prisco, R. (eds.) *SCN 2014*. LNCS, vol. 8642, pp. 514–519. Springer, Heidelberg (2014)
14. Catalano, D., Marcedone, A., Puglisi, O.: Authenticating computation on groups: new homomorphic primitives and applications. In: Sarkar, P., Iwata, T. (eds.) *ASIACRYPT 2014, Part II*. LNCS, vol. 8874, pp. 193–212. Springer, Heidelberg (2014)
15. Chase, M., Kohlweiss, M., Lysyanskaya, A., Meiklejohn, S.: Malleable signatures: new definitions and delegatable anonymous credentials. In: *CSF*, pp. 199–213. IEEE (2014)
16. Cloud Security Alliance: Cloud security alliance website (2009). <https://cloudsecurityalliance.org>. Accessed 31 March 2015
17. Danezis, G., Kohlweiss, M., Rial, A.: Differentially private billing with rebates. In: Filler, T., Pevný, T., Craver, S., Ker, A. (eds.) *IH 2011*. LNCS, vol. 6958, pp. 148–162. Springer, Heidelberg (2011)
18. Di Lorenzo, G., Hacid, H., Benatallah, B., Paik, H.Y.: Data integration in mashups. *Sigmod Rec.* **38**(1), 59–66 (2009)
19. Erl, T.: *Service-Oriented Architecture: Concepts, Technology, and Design*. Pearson Education India, Delhi (2006)
20. 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>. Accessed 31 March 2015
21. European Union Agency for Network and Information Security-ENISA: Cloud computing repository. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing>
22. Fiore, D., Gennaro, R., Pastro, V.: Efficiently verifiable computation on encrypted data. In: *ACM CCS*, pp. 844–855 (2014)
23. Ghernaouti-Helie, S.: *Cyber Power - Crime. Conflict and Security in Cyberspace*. EPFL Press, Burlington (2013)

24. Groß, T.: Signatures and efficient proofs on committed graphs and NP-statements. In: Böhme, R., Okamoto, T. (eds.) FC 2015. LNCS, vol. 8975, pp. 293–314. Springer, Heidelberg (2015)
25. Gupta, V.H., Gopinath, K.: G_{its}^2 vsr: an information theoretical secure verifiable secret redistribution protocol for long-term archival storage. In: Security in Storage Workshop, SISW 2007, pp. 22–33. IEEE Computer Society, Washington, DC, USA (2007). <http://dx.doi.org/10.1109/SISW.2007.9>
26. Hanser, C., Slamanig, D.: Blank digital signatures. In: ASIA CCS. ACM (2013)
27. Hanser, C., Slamanig, D.: Structure-preserving signatures on equivalence classes and their application to anonymous credentials. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 491–511. Springer, Heidelberg (2014)
28. Harbach, M., Fahl, S., Rieger, M., Smith, M.: On the acceptance of privacy-preserving authentication technology: the curious case of national identity cards. In: De Cristofaro, E., Wright, M. (eds.) PETS 2013. LNCS, vol. 7981, pp. 245–264. Springer, Heidelberg (2013)
29. Johnson, R., Molnar, D., Song, D., Wagner, D.: Homomorphic signature schemes. In: Preneel, B. (ed.) CT-RSA 2002. LNCS, vol. 2271, pp. 244–262. Springer, Heidelberg (2002)
30. Moran, T., Naor, M.: Split-ballot voting: everlasting privacy with distributed trust. ACM Trans. Inf. Syst. Secur. **13**(2), 246–255 (2010)
31. Müller-Quade, J., Unruh, D.: Long-term security and universal composability. J. Cryptol. **23**(4), 594–671 (2010)
32. National Institute of Standards and Technology-NIST: Cloud computing program. <http://www.nist.gov/itl/cloud/index.cfm>. Accessed 31 March 2015
33. Paquin, C., Zaverucha, G.: U-prove cryptographic specification v1.1, revision 3. Technical report, Microsoft Corporation (2013)
34. Pfeffer, H., Linner, D., Steglich, S.: Modeling and controlling dynamic service compositions. In: Computing in the Global Information Technology, pp. 210–216. IEEE (2008)
35. Pöhls, H.C., Samelin, K.: On updatable redactable signatures. In: Boureanu, I., Owesarski, P., Vaudenay, S. (eds.) ACNS 2014. LNCS, vol. 8479, pp. 457–475. Springer, Heidelberg (2014)
36. 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>. Accessed 31 March 2015
37. Schiffman, J., Sun, Y., Vijayakumar, H., Jaeger, T.: Cloud verifier: verifiable auditing service for IaaS clouds. In: CSA, June 2013
38. Slamanig, D.: Efficient schemes for anonymous yet authorized and bounded use of cloud resources. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 73–91. Springer, Heidelberg (2012)
39. Slamanig, D., Hanser, C.: On cloud storage and the cloud of clouds approach. In: ICITST-2012, pp. 649–655. IEEE Press (2012)
40. Steinfeld, R., Bull, L., Zheng, Y.: Content extraction signatures. In: Kim, K. (ed.) ICISC 2001. LNCS, vol. 2288, p. 285. Springer, Heidelberg (2002)
41. 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>. Accessed 31 March 2015
42. Walfish, M., Blumberg, A.J.: Verifying computations without reexecuting them. Commun. ACM **58**(2), 74–84 (2015)
43. Wästlund, E., Angulo, J., Fischer-Hübner, S.: Evoking comprehensive mental models of anonymous credentials. In: iNetSec, pp. 1–14 (2011)

Cyber Security and Privacy

4th Cyber Security and Privacy Innovation Forum, CSP
Innovation Forum 2015, Brussels, Belgium April 28-29,
2015, Revised Selected Papers

Cleary, F.; Felici, M. (Eds.)

2015, XVI, 151 p. 29 illus. in color., Softcover

ISBN: 978-3-319-25359-6