Cloud Cryptography: Theory, Practice and Future Research Directions

Kim-Kwang Raymond Choo, University of South Australia, Australia
Email: Raymond.Choo@unisa.edu.au

Josep Domingo-Ferrer, Universitat Rovira i Virgili, Catalonia
Email: josep.domingo@urv.cat

Lei Zhang, East China Normal University, China
Email: leizhang@sei.ecnu.edu.cn

1. Introduction

Cloud computing, a convenient way of accessing services, resources and applications over the Internet, shifts the focus of industries and organizations away from the deployment and day-to-day running of their IT facilities by providing an on-demand, self-service, and pay-as-you-go business model. It is, therefore, unsurprising that cloud computing has continued to increase in popularity in recent times.

While cloud computing provides various benefits to users, there are underlying security and privacy risks. For example, multi-tenancy, resource pooling and shareability features can be exploited by cybercriminals and anyone with a malicious intent, to the detriment of both cloud users and cloud service providers. It is unsurprising, then, that cloud computing has emerged as a salient area of inquiry for security researchers. For example, when user data (e.g. documents, videos and photos) are uploaded or stored in a cloud computing service, the data owners are unlikely to know the path of the transmitted data or whether the data are being collected and analyzed by a third party, including a government agency (see the revelations by Edward Snowden – European Parliament 2014). As posited by Choo and Sarre (2015), it is important to strike a balance between privacy, legitimate surveillance and lawful data access, in order to ensure that the privacy of innocent individuals will not be compromised (e.g. that fine-grained aspects of an individual's life cannot be derived or inferred from the intelligence collection and analysis).

A particularly promising approach to achieve security and privacy in this new computing paradigm is through cryptography (Qin et al. 2013; Wang et al. 2014). For example, as noted by Yang et al. (2015), to ensure the security and privacy of user data, specifically against an untrusted cloud service provider, one could encrypt the data prior to uploading and storing the data in the cloud.

This special issue is dedicated to providing both scientists and practitioners with a forum to present their recent research on the use of novel cryptographic techniques to improve the security and privacy of the underlying cloud architecture or ecosystem, particularly research that integrates both theory and practice. For example, how do we design an efficient cloud cryptography system that offers enhanced security and/or privacy without compromising on usability and performance? In the sequel, we briefly survey the content of papers in this special issue.

2. Fully homomorphic encryption and searchable encryption

A fully homomorphic encryption scheme enables computations to be carried out on ciphertext. Such a scheme guarantees that the cloud service provider is unable to view the content of the data he stores (thereby ensuring user data confidentiality/privacy). However, sufficiently efficient fully homomorphic encryption is not yet available, as noted by Wang, Malluhi and Khan (2016). In their article entitled “Garbled computation in cloud”, they propose a weaker/relaxed privacy definition in their design of efficient reusable garbled circuits. The latter can then be used to more efficiently process encrypted cloud data.

Searchable encryption schemes are another research focus in recent years – see Han, Qin and Hu (2016) and Renwick and Martin (2016) for a review of recent advances. In the review of Renwick and Martin (2016), existing challenges that need to be overcome in order to ensure that such schemes are deployable on practical systems are also discussed. Searchable symmetric encryption (SSE – Curtmola et al. 2006) is one example of a searchable encryption scheme. Dai, Li and Zhang (2016) present a formal definition for memory leakage resilient SSE, prior to proposing an adaptive memory leakage resilient SSE scheme and a non-adaptive dynamic memory leakage resilient SSE scheme based on physical unclonable functions (PUFs).

3. Data integrity

Ensuring the integrity of data outsourced to the cloud is as important as ensuring the security and privacy of user data. Solutions based on public-key infrastructure generally suffer from key management issues, and seeking to address the limitations associated with such an approach, Yu et al. (2016) propose an identity-based cloud data integrity checking protocol and prove its security. Using a different approach, Hu, Lo and Chen (2016) propose an image authentication scheme that allows detecting areas having been tampered with for image demosaicking with the reversibility-preserving property.

Aspnes et al. (2007) adapted the data entanglement (initially designed to increase censorship resistance in document storage systems) to protect data from an untrusted (cloud) storage provider who may be motivated to damage or destroy the data. As noted by Ateniese et al. (2016), the revised data entanglement approach of Aspnes et al. (2007) relies on a trusted authority in file retrieval. Seeking to address this limitation, Ateniese et al. (2016) present a simulation-based definition of security for entangled cloud storage whose security is proven in the universal composability model. They then design a protocol implementing the ideal functionality for entangled storage.

4. Data sharing

Data sharing in an untrusted or semi-trusted cloud environment is also a subject of recent research focus. To achieve fine-grained data sharing in a cloud environment, one could deploy schemes such as ciphertext-policy attribute-based conditional proxy re-encryption (Yang et al. 2016) and online/offline attribute-based proxy re-encryption (Shao, Lu and Lin 2015). In this special issue, Canard and Devigne (2016) demonstrate how existing proxy re-encryption schemes can be modified in order for users to dynamically manage a tree structure for their shared document. They then demonstrate the utility of the approach using a prototype implementation. Another data sharing scheme is presented by Zhou et al. (2016), who propose an identity-based proxy re-encryption version 2. The latter is designed to allow an authorized proxy to convert a ciphertext from an identity-based broadcast encryption scheme to a ciphertext of an identity-based encryption scheme. Lu and Li (2016) also present a certificate-based proxy re-encryption scheme without bilinear pairings, in order to share encrypted data in public clouds.

There are situations where data owners wish to share their data for a pre-determined period, and existing remote wiping and secure deletion mechanisms, such as those for mobile devices (Leom, Choo and Hunt 2016), may not be fit-for-purpose in a cloud environment. Huang, Fan and Tseng (2016) explain how their proposed enabled/disabled predicate encryption scheme can be used to provide timed-release services and data self-destruction. In other words, a data owner can preset the readable/unreadable time of the files prior to sending them to the receiver.

5. Skyline computation

Skyline computation allows a user to obtain a set of interesting points from a big data space, thus informing multi-criteria decision making and client preference applications. However, there are various security and privacy considerations. In this special issue, Liu et al. (2016) propose a privacy-preserving skyline computation framework designed for cross-domain searches. In other words, skyline set processing performed by a domain will not result in leakage of data to other domains.

6. Trust evaluation

Trust management is a crucial component in any technologies, and cloud computing is no exception. Yan et al. (2016) observe the lack of research on privacy-preserving trust evaluation, also in a cloud computing context. The authors then propose two schemes based on additive homomorphic encryption to ensure the privacy of trust evidence providers.

7. Mobile cloud

With the increasing popularity of smart mobile devices (e.g. smart phones), for example in accessing cloud services, mobile cloud computing is a topic that has received attention from both researchers and industry. As noted by Yang, Huang and Liu (2016), in a mobile cloud environment, the capability to support seamless roaming and secure handover is crucial to ensure quality of service and security. However, this is challenging task due to the different heterogeneous distributed systems. In their paper, a handoff authentication for heterogeneous mobile cloud networks is proposed, which is designed to provide both user anonymity and untraceability.

An efficient batch public key cryptosystem is particularly suited for resource-limited environment, such as mobile cloud. Wu et al. (2016) explain how batch multi-exponentiations can be expedited under different configurations and present a batch public key cryptosystem scheme based on the Cramer–Shoup cryptosystem.

8. Future research directions

Despite the amount of research efforts to ensure the security, privacy and integrity of cloud data and services, there are a number of challenges that remain to be addressed. For example, is it possible to design technologies that are robust in the sense that their legitimate use is minimally constrained, but their illegitimate use is prevented or discouraged (Choo 2011; Grabosky 2007)? A recent survey also identified the need for an efficient defense solution that can be deployed in practice to detect both application-bug level and infrastructural level distributed denial of service (DDoS) attacks (Osanaiye, Choo and Dlodlo 2016).

Also worth exploring are non-cryptographic solutions allowing secure and privacy-preserving storage and processing of data in semi-honest clouds. Avoiding cryptography results in lighter computations while still providing an acceptable privacy level in some scenarios. In the European H2020 project "CLARUS" (2015-2017) both cryptographic and non-cryptographic approaches are investigated. Among the latter, Calviño, Ricci and Domingo-Ferrer (2015) present methods for statistical data computation on data split across different clouds. Challenges along this line include expanding the range of feasible computations on split data, and also finding alternatives to split data as a way to allow non-cryptographic privacy-preserving cloud data processing.

References

James Aspnes, Joan Feigenbaum, Aleksandr Yampolskiy, Sheng Zhong 2007. Towards a theory of data entanglement. *Theoretical Computer Science* 389(1-2): 26-43

Giuseppe Ateniese, Ozgur Dagdelen, Ivan Damgård, Daniele Venturi 2016. Entangled cloud storage. *Future Generation Computer Systems* http://dx.doi.org/10.1016/j.future.2016.01.008

Aida Calviño, Sara Ricci and Josep Domingo-Ferrer 2015. Privacy-preserving distribution of statistical computation to a semi-honest multi-cloud. In 2015 IEEE Conference on Communications and Network Security (CNS 2015), Florence, Italy, Sep. 28-30. IEEE, pp. 506-514.

Sébastien Canard, Julien Devigne 2016. Highly privacy-protecting data sharing in a tree structure. *Future Generation Computer Systems*

Kim-Kwang Raymond Choo 2011. The cyber threat landscape: challenges and future research directions. *Computers & Security* 30(8): 719-731

Kim-Kwang Raymond Choo, Rick Sarre 2015. Balancing privacy with legitimate surveillance and lawful data access. *IEEE Cloud Computing* 2(4): 8-13

Reza Curtmola, Juan Garay, Seny Kamara, Rafail Ostrovsky 2006. Searchable symmetric encryption: improved definitions and efficient constructions. In Proceedings of the 13th ACM

Conference on Computer and Communications Security (ACM CCS 2006), pp. 79-88

European Parliament 2014. Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs. *Plenary Sitting*. http://www.europarl.europa.eu/document/activities/cont/201403/20140306ATT80632/20140306ATT80632EN.pdf

Shuguang Dai, Huige Li, Fangguo Zhang 2016. Memory leakage-resilient searchable symmetric encryption. *Future Generation Computer Systems* http://dx.doi.org/10.1016/j.future.2015.11.003

Peter Grabosky 2007. The internet, technology, and organized crime. *Asian Journal of Criminology* 2(2):145e61

Fei Han, Jing Qin, Jiankun Hu 2016. Secure searches in the cloud: a survey. *Future Generation Computer Systems*

Yu-Chen Hu, Chun-Chi Lo, and Wu-Lin Chen 2016. Probability-based reversible image authentication scheme for image demosaicking. *Future Generation Computer Systems*

Shi-Yuan Huang, Chun-I Fan, Yi-Fan Tseng 2016. Enabled/disabled predicate encryption in clouds. *Future Generation Computer Systems* http://dx.doi.org/10.1016/j.future.2015.12.008

Ming Di Leom, Kim-Kwang Raymond Choo, Ray Hunt 2016. Remote wiping and secure deletion on mobile devices: A review. *Journal of Forensic Sciences* [In press]

Ximeng Liu, Rongxing Lu, Jianfeng Ma, Le Chen, Haiyong Bao 2016. Efficient and privacy-preserving skyline computation framework across domains. *Future Generation Computer Systems* http://dx.doi.org/10.1016/j.future.2015.10.005

Yang Lu, Jiguo Li 2016. A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds. *Future Generation Computer Systems* http://dx.doi.org/10.1016/j.future.2015.11.012

Opeyemi Osanaiye, Kim-Kwang Raymond Choo, Mqhele Dlodlo 2016.
Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. *Journal of Network and Computer Applications*

http://dx.doi.org/10.1016/j.jnca.2016.01.001

Sarah Louise Renwick, Keith M. Martin 2016. Practical architectures for deployment of searchable encryption in a cloud environment. *Future Generation Computer Systems*

Jun Shao, Rongxing Lu, Xiaodong Lin 2015. Fine-grained data sharing in cloud computing for mobile devices. In Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM 2015), pp. 2677-2685.

Bo Qin, Huaqun Wang, Qianhong Wu, Jianwei Liu, Josep Domingo-Ferrer 2013. Simultaneous authentication and secrecy in identity-based data upload to cloud. *Cluster Computing* 16(4): 845-859

Yongge Wang, Qutaibah M. Malluhi, Khaled MD Khan 2016. Garbled computation in cloud. *Future Generation Computer Systems* http://dx.doi.org/10.1016/j.future.2015.11.004

Huaqun Wang, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer 2014. Identity-based remote data possession checking in public clouds. *IET Information Security* 8(2): 114-121

Qianhong Wu, Yang Sun, Bo Qin, Jiankun Hu, Weiran Liu, Jianwei Liu, Yong Ding 2016. Batch public key cryptosystem with batch multi-exponentiation. *Future Generation Computer Systems* http://dx.doi.org/10.1016/j.future.2015.12.009

Zheng Yan, Wenxiu Ding, Valtteri Niemi, Athanasios V. Vasilakos 2016. Two schemes of privacy-preserving trust evaluation. *Future Generation Computer Systems* http://dx.doi.org/10.1016/j.future.2015.11.006

Xu Yang, Xinyi Huang, Joseph K. Liu 2016. Efficient handover authentication with user anonymity and untraceability for mobile cloud computing. *Future Generation Computer Systems* http://dx.doi.org/10.1016/j.future.2015.09.028

Yanjiang Yang, Joseph K. Liu, Kaitai Liang, Kim-Kwang Raymond Choo, Jianying Zhou 2015. Extended proxy-assisted approach: achieving revocable fine-grained encryption of cloud data. In Proceedings of 20th European Symposium on Research in Computer Security (ESORICS 2015), Vienna, Austria, Volume 9327/2015 of Lecture Notes in Computer Science (pp. 146 - 166), Springer-Verlag, 21–25 September

Yanjiang Yang, Haiyan Zhu, Haibing Lu, Jian Weng, Youcheng Zhang, Kim-Kwang

Raymond Choo 2016. Cloud based data sharing with fine-grained proxy re-encryption. *Pervasive and Mobile Computing* http://dx.doi.org/10.1016/j.pmcj.2015.06.017

Yong Yu, Liang Xue, Man Ho Au, Willy Susilo, Jianbing Ni, Yafang Zhang, Athanasios V. Vasilakos, Jian Shen 2016. Cloud data integrity checking with an identity-based auditing mechanism from RSA. *Future Generation Computer Systems*

Yunya Zhou, Hua Deng, Qianhong Wu, Bo Qin, Jianwei Liu, Yong Ding 2016. Identity-based proxy re-encryption version 2: Making mobile access easy in cloud. *Future Generation Computer Systems* http://dx.doi.org/10.1016/j.future.2015.09.027