Cloud Security Engineering: Theory, Practice and Future Research

Kim-Kwang Raymond Choo, Omer F. Rana, and Muttukrishnan Rajarajan

1 Introduction

As the use of cloud computing grows throughout society in general, it is essential that cloud service providers and cloud service users ensure that security and privacy safeguards are in place. There is, however, no perfect security and when a security incident involving cloud services occurs, digital investigation will require the identification, preservation and analysis of evidential data [3], [24]. Therefore, it is unsurprising that cloud security has seen significant research interest recently [2], [5], [13], [30].

This special issue is dedicated to the identification of techniques that enable security mechanisms to be engineered and implemented in cloud services and cloud systems. A key focus is on the integration of theoretical foundations with practical deployment of security strategies that make cloud systems more secure for both end users and providers – enabling end users to increase the level of trust they have in cloud service providers – and conversely for cloud service providers to provide greater guarantees to end users about the security of their services and data. To meet particular Quality of Service targets, Cloud providers have made large investments in: (i) improving application performance for end users; (ii) enable differentiation of capability by providing support for specialist hardware infrastructure (such as GPUs or dedicated network between virtual machines); (iii) improving Power Usage Effectiveness (PUE) ratings to make more efficient use of energy (saving both energy costs and reducing environmental impact). This special issue is dedicated to understanding whether a similar engineering philosophy can be extended to support security mechanisms, and more importantly, whether experience from the performance engineering community (who often need to carry out analysis on large log files) can be carried over into the security domain?

We received 44 submissions for this special issue, of which 11 have been accepted. Each paper went through a rigorous peer review process, in addition to multiple follow-up rounds with the authors. A summary of the papers and their placement in the wider cloud security context is provided below.

- *K.-K.R. Choo is with the University of Texas at San Antonio, San Antonio, TX 78249, and also with the University of South Australia, Adelaide, SA 5001, Australia. E-mail: raymond.choo@fulbrightmail.org.*
- *O.F. Rana is with Cardiff University, Cardiff, CF 10 3XQ, United Kingdom. E-mail: RanaOF@cardiff.ac.uk.*
- *M. Rajarajan is with City University London, London EC1V 0HB, United Kingdom. E-mail: r.muttukrishnan@city.ac.uk.*

For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TCC.2016.2582278

2 Security

Varadharajan and Tupakula (2016) present a security architecture, which integrates policy based access control, intrusion detection techniques and trusted computing technologies. They then demonstrate how the architecture can be used to secure the life cycle of virtual machines and migration of virtual machines across different physical servers. Similarly, Xia et al. (2016) present an integrated hardware and software approach to ensure the security of a cloud user's virtual machine when the computations are outsourced to the cloud.

Paladi, Gehrmann, and Michalas (2016) describe a framework for data and operation security in the Infrastructure as a Service (IaaS) model. The security and efficiency of the underlying protocols are then demonstrated. The utility of the framework prototype is also shown in a prototype implementation in an electronic health record system context. Seeking to contribute to the challenge of assessing the likelihood of malicious coresidency in public cloud services, Ezhilchelvan and Mitrani (2016) present two allocation policies for assigning virtual machines to servers.

Nepal et al. (2016) present a trusted storage cloud for scientific workflows (TruXy) and the underlying protocols. They then demonstrate how TruXy can be deployed to support collaborative bioinformatics research (i.e., processing of exome datasets of individuals with rare genetic disorders).

The use of Service Level Agreements (SLAs) are one common strategy undertaken by cloud service users, particularly organizational users, to ensure Quality of Service and other requirements are in place. Esposito, Castiglione and Choo (2016), for example, remarked that ensuring data sovereignty can also be part of the SLA management system. This is also echoed by Luna et al. (2016) in this special issue, who emphasized the importance of including security specifications in SLAs (i.e., the development of security level agreements). They then present two evaluation techniques to conduct quantitative assessment and analysis of metrics included within a security level agreement with respect to pre-agreed security requirements. Both techniques are also validated using two use case scenarios and a prototype, with real world data from Cloud Security Alliance's Security, Trust and Assurance Registry. This aspect also aligns with recent interest in auditing security capability of a cloud provider – for instance in the European "Cloud Accountability" (A4Cloud) project.

Understanding how security credentials of a cloud provider could be audited through operational data collection (referred to as "evidence" in A4Cloud), especially by a third party, remains an important challenge.

3 Privacy (Includes Data Access and Data Sharing)

Ensuring the privacy of user data and computations is a crucial component in any technology which involves data outsourcing, including cloud computing, and user data can potentially be the subject of surveillance [6], [23]. One high profile incident involved the leakage of multimedia contents stored in the cloud in September 2014, where a number of celebrity's iCloud accounts were reportedly compromised. Consequently, intimate photos were stolen from these compromised accounts [10], [11], [26], and the incident was subsequently confirmed by Apple (2014).

Thus, privacy protection and preservation are equally important for cloud users and unsurprisingly, data sharing and data access in an untrusted or semi-trusted cloud environment have been the focus of recent research efforts (see [4], [14], [16], [31]). Data sharing and data access are also examined by Pasquier et al. (2016) and Yan et al. (2016) in this special issue. Specifically, Pasquier et al. (2016) present the Cambridge Flow Control Architecture (CamFlow) designed to enforce data flow policy and reduce the potential for data leakage due to malicious or buggy software, and Yan et al. (2016) present a data access scheme which employs both attribute-based encryption and proxy re-encryption.

Searchable encryption schemes are also a subject of recent research focus – see Han, Qin and Hu (2016). In this special issue, Li et al. (2016) propose a mechanism design to ensure the security and privacy of searchable encrypted data outsourced to the cloud. Specifically, their approach allows a cloud user to distribute their encrypted data across multiple cloud services, as well as the ability to conduct search on these data. The practicality of the approach is demonstrated using Amazon EC2 and a real world dataset.

4 Forensics

Our increased dependence on technologies, including cloud services, can potentially expose us to a wide range of nefarious activities such as hacking, theft of intellectual property and trade secrets, and online child exploitation. Every electronic/digital action leaves an evidence trail, for example, on client devices, cloud servers, within the generated network traffic, etc. Consequently, there is a growing need for forensic investigations to ascertain how an attack was carried out or how an event occurred on a cloud service. This is the gap that Ma et al. (2016) and Qi et al. (2016) seek to address.

Ma et al. (2016) introduce a fully reversible privacy region protection for cloud video surveillance based on their proposed fully reversible privacy protection method for H.264/AVC compressed video. Qi et al. (2016) present a tool designed to acquire and preserve data in a cloud computing environment.

5 Where to Go from Here?

Despite the significant amount of research published in addressing security, privacy and forensic issues relating to the use of cloud services, there are a number of challenges that remain to be addressed. Recent surveys, for example, identified the need for effective and efficient defense solutions that can be deployed in practice to detect both application-bug level and infrastructural level distributed denial of service attacks [18], [21].

Potential topics for future research would include:

- Advanced security features
- Anonymity
- Cloud forensic and anti-forensic techniques and implementations
- Cloud privacy
- Cloud-based honeypots
- Cloud-based intrusion detection and prevention systems
- Distributed authentication and authentication
- Implementation of cryptographic and key management strategies in clouds (e.g. homomorphic encryption for cloud computing)
- Multi-Cloud security provisioning
- Privacy preserving data mining
- Searchable encryption
- Multi-party computation
- Real time analysis of security (log) data for alert generation
- Remote collection of evidence (e.g. from cloud servers)
- Security-focused Service Level Agreements, cloud auditing & certification
- User-based security monitoring for Virtual Machines and Containers.

We hope the articles in this special issue provide useful insights into engineering security for cloud systems.

References

[1] Apple, Apple Media Advisory: Update To Celebrity Photo Investigation, Sept. 2, 2014. [Online]. Available: http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html

[2] T. Al Said and O. F. Rana, "Analysing virtual machine security in cloud systems," in *Proc. Int. Conf. Intell. Cloud Comput.*, 2014, pp. 137–151.

[3] N. H. Ab Rahman and K.-K. R. Choo, "A survey of information security incident handling in the cloud," *Comput. Secur.*, vol. 49, no. C, pp. 45–69, 2015.

[4] S. Canard and J. Devigne, "Highly privacy-protecting data sharing in a tree structure," *Future Gener. Comput. Syst.*, vol. 62, pp. 119–127, Sep. 2016.

[5] K.-K. R. Choo, J. Domingo-Ferrer, and L. Zhang, "Cloud cryptography: Theory, practice and future research directions," *Future Gener. Comput. Syst.*, vol. 62, pp. 51–53, 2016.

[6] K.-K. R. Choo and R. Sarre, "Balancing privacy with legitimate surveillance and lawful data access," *IEEE Cloud Comput.*, vol. 2, no. 4, pp. 8–13, Jul./Aug. 2015.

[7] C. Esposito, A. Castiglione, and K.-K. R. Choo, "Encryption-based solution for data sovereignty in federated clouds," *IEEE Cloud Comput.*, vol. 3, no.1, pp. 12–17, Jan./Feb. 2016.

[8] P. Ezhilchelvan and I. Mitrani, "Evaluating the probability of Malicious co-residency in public clouds," *IEEE Trans. Cloud Comput.*, to be published; Doi: 10.1109/TCC.2015.2451633.

[9] F. Han, J. Qin, and J. Hu, "Secure searches in the cloud: A survey," *Future Gen. Comput. Syst.*, vol. 62, pp. 66–75, 2016.

[10] L. Kelion, (2014). "Apple toughens iCloud security after celebrity breach," *BBC News* 17 Sep. [Online]. Available: http://www.bbc.com/news/technology-29237469
[11] D. Lewis, (2014), "iCloud Data Breach: Hacking and Celebrity Photos". *Forbes* 2 Sep. [Online]. Available: http://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos/
[12] J. Li, D. Lin, A. Squicciarini, J. Li, and C. Jia, "Towards privacy-preserving storage and retrieval in multiple clouds," *IEEE Trans. Cloud Comput.*, 2016, to be published; Doi: 10.1109/TCC.2015.2485214.
[13] F. Li, Y. Rahulamathavan, M. Conti, and M. Rajarajan, "Robust access control framework for mobile cloud computing network," *Comput. Commun.*, vol. 68, pp. 61–72, 2015.
[14] Y. Lu and J. Li, "A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds," *Future Gen. Comput. Syst.*, vol. 62, pp. 140–147, 2016.
[15] J. Luna, A. Taha, R. Trapero, and N. Suri, "Quantitative reasoning about cloud security using service level agreements," *IEEE Trans. Cloud Comput.*, 2016, to be published; Doi: 10.1109/TCC.2015.2469659.
[16] X. Ma, L. T. Yang, Y. Xiang, W. Zeng, D. Zou, and H. Jin, "Fully reversible privacy region protection for cloud video surveillance," *IEEE Trans. Cloud Comput.*, 2016, to be published; Doi: 10.1109/TCC.2015.2469651.
[17] S. Nepal, et al., "TruXy: Trusted storage cloud for scientific workflows," *IEEE Trans. Cloud Comput.*, 2016, Doi: 10.1109/TCC.2015.2489638.
[18] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework," *J. Netw. Comput. Appl.*, vol. 67, pp. 147–165, 2016.
[19] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," *IEEE Trans. Cloud Comput.*, 2016, to be published; Doi: 10.1109/TCC.2016.2525991.
[20] T. F. J.-M. Pasquier, J. Singh, D. Eyers, and J. Bacon, "CamFlow: Managed data-sharing for cloud services," *IEEE Trans. Cloud Comput.*, 2016, to be published; Doi: 10.1109/TCC.2015.2489211.
[21] V. Prokhorenko, K.-K. R. Choo, and H. Ashman, "Web application protection techniques: A taxonomy," *J. Netw. Comput. Appl.*, vol. 60, pp. 95–112, 2016.
[22] Z. Qi, C. Xiang, R. Ma, J. Li, H. Guan, and D. S. L. Wei, "ForenVisor: A tool for acquiring and preserving reliable data in cloud live forensics," *IEEE Trans. Cloud Comput.*, 2016, to be published; Doi: 10.1109/TCC.2016.2535295.
[23] D. Quick and K.-K. R. Choo, "Big forensic data reduction: Digital forensic images and electronic evidence," *Cluster Comput.*, vol. 19, no. 2, pp. 723–740, 2016.
[24] D. Quick, B. Martini, and K.-K. R. Choo, *Cloud Storage Forensics*. MA, USA: Syngress Publishing / Elsevier, 2013.
[25] V. Varadharajan and U. Tupakula, "On the design and implementation of an integrated security architecture for cloud with improved resilience," *IEEE Trans. Cloud Comput.*, 2016, to be published; Doi: 10.1109/TCC.2016.2535320.
[26] D. Wakabayashi and D. Yadron, (2014), "Apple denies iCloud breach," *The Wall Street Journal* 2 Sep., [Online]. Available http://online.wsj.com/articles/apple-celebrity-accounts-compromised-by-very-targeted-attack-1409683803
[27] Y. Xia, et al., "Secure outsourcing of virtual appliance," *IEEE Trans. Cloud Comput.*, 2016, to be published; Doi: 10.1109/TCC.2015.2469657.
[28] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," *IEEE Trans. Cloud Comput.*, 2016, to be published; Doi: 10.1109/TCC.2015.2469662.
[29] Y. Yang, J. K. Liu, K. Liang, K.-K. R. Choo, and J. Zhou, "Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," in *Proc. 20th Eur. Symp. Res. Comput. Security*, vol. 9327, 2015, pp. 146–166.
[30] Y. Rahulamathavan, R. C.-W. Phan, S. Veluru, K. Cumanan, M. Rajarajan, "Privacy-preserving multi-class support vector machine for outsourcing the data classification in cloud," *IEEE Trans. Depend. Secure Comput.*, vol. 11, no. 5, pp. 467–479, Sep./Oct. 2014.
[31] Y. Zhou, H. Deng, Q. Wu, B. Qin, J. Liu, and Y. Ding, "Identity-based proxy re-encryption version 2: Making mobile access easy in cloud," *Future Gen. Comput. Syst.*, vol. 62, pp. 128–139, 2016.