Ann. Telecommun. (2017) 72:233–235
DOI 10.1007/s12243-017-0578-3

EDITORIAL

Security and privacy issues in cloud computing

Haider Abbas[1,2] · Olaf Maennel[3] · Saïd Assar[4]

Published online: 21 April 2017

Cloud computing is a state-of-the-art technological innovation providing an extensive list of benefits for almost every business and governmental, small or medium-sized organizations. It has truly revolutionized the computational era by cutting down cost and reducing complexities of infrastructural configurations for computational platforms. This state-of-the-art technology is rapidly being adapted by various large organizations from healthcare to critical infrastructure to carry out their business processes that, otherwise, would require large storage capacity, huge computational power, and expensive hardware.

On the other hand, this technological advent also introduces novel ways of information leakage and user classified data security and privacy issues since data is stored and transmitted over the cloud and even across borders. This seems very threatening to the cloud user's community, and they have raised very serious concerns about these issues. Although extensive research efforts have been carried out to address data security and privacy issues in cloud-assisted systems, this still requires many more efforts to counter these issues effectively.

The purpose of this special issue was to arrange a venue for cloud researchers around the world to share their state-of-the-art research and development that could benefit the cloud community. This helped collect high-quality articles that reported recent research advances regarding security and privacy issues in cloud computing, covering various topics of interest. We received 26 articles, and each article was rigorously reviewed by at least three experts. Finally, we selected 11 articles for publication. The brief descriptions of the selected articles are presented below.

The paper entitled "Service resizing for quick DDoS mitigation in cloud computing environment" by Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, and Rajkumar Buyya presents important metrics to evaluate the performance of a DDoS mitigation process in the cloud computing environment[1]. The authors propose a novel framework consisting of an affinity-based victim-service resizing algorithm to provide performance isolation and a TCP-tuning technique to quickly free the attack connections, hence minimizing the attack cooling down period. Extensive real attack experiments show a significant improvement in the performance of the DDoS mitigation service, providing quick attack mitigation.

The paper entitled "An empirical study on acceptance of secure healthcare service in Malaysia, Pakistan, and Saudi Arabia: a mobile cloud computing perspective" by Rooh ul Amin, Irum Inayat, Basit Shahzad, Kashif Saleem, and Li Aijun conducted an empirical study to investigate the behavioral intention of healthcare organizations' staff towards the usage of cloud-based healthcare services to carry out their daily jobs in Malaysia, Pakistan, and Saudi Arabia[2]. The results showed that social influence was the least influencing predictor in determining the dependent variable and that the years of experience positively influenced the user's behavioral intentions towards using cloud-based healthcare services.

✉ Haider Abbas
dr.h.abbas@ieee.org

Olaf Maennel
olaf.maennel@ttu.ee

Saïd Assar
said.assar@telecom-em.eu

[1] National University of Sciences and Technology, Islamabad, Pakistan

[2] Florida Institute of Technology, Melbourne, FL, USA

[3] Tallinn University of Technology, Tallinn, Estonia

[4] Télécom École de Management, Évry, France

The paper entitled "Securing wireless sensor networks for improved performance in cloud-based environments" by Ashfaq Hussain Farooqi and Farrukh Aslam Khan presents the approach by modifying the low-energy adaptive clustering hierarchy (LEACH) protocol for wireless sensor networks (WSNs) and adding the functionality of intrusion detection to secure WSNs from sinkhole, black hole, and selective forwarding attacks[3]. The modified protocol was called LEACH++. They performed two types of analyses: numerical analysis to check the effect on throughput and energy, and simulations in Network Simulator-2 (NS-2) to prove the results found from the numerical analysis. The results they showed were quite promising and favor LEACH++ over LEACH under attack with respect to throughput and energy consumption.

The paper entitled "Attacks and countermeasures in the Internet of Vehicles" by Yunchuan Sun, Lei Wu, Shizhong Wu, Shoupeng Li, Tao Zhang, Li Zhang, Junfeng Xu, Yongping Xiong, and Xuegang Cui presents a review of the advances on issues of security and privacy in the cloud-assisted Internet of Vehicles (IoV), including security and privacy requirements, attack types, and the relevant solutions, and discussed challenges and future trends in this area[4].

The paper entitled "Modeling network traffic for traffic matrix estimation and anomaly detection based on Bayesian network in cloud computing networks" authored by Laisen Nie, Dingde Jiang, and Zhihan Lv proposed a Bayesian network-based traffic matrix estimation approach that can also be used to implement anomaly detection[5]. The proposed method was evaluated and consistently outperformed three state-of-the-art methods in estimation bias.

The paper entitled "EACF: extensible access control framework for cloud environments" authored by Faria Mehak, Rahat Masood, Muhammad Awais Shibli, and Islam Elgedway presents an extensible access control framework (EACF) for cloud-based applications, which provided high-level extensibility by incorporating different access control models about the needs of the cloud service consumers (organizations)[6]. They also presented a case study in which three access control models were incorporated into the framework and tested on SaaS-hosted application DSpace to ascertain that the proposed features are functional and working efficiently.

The paper entitled "Security and management framework for an organization operating in cloud environment" by Nasir Raza, Imran Rashid, and Fazeel Ali Awan proposed a comprehensive security and management framework for an organization operating in the cloud environment[7]. The proposed framework was implemented in a virtualized cloud environment, and the results were presented in the article to validate the efficacy of certain features of the model.

The paper entitled "Software defined systems support for secure cloud computing based on data classification" authored by Yaser Jararweh, Mahmoud Al-Ayyoub, Lo'ai Tawalbeh, Ala' Darabseh, and Houbing Song presents a software-defined system-based solution for deploying an efficient data classification framework[8]. They also showed the significance of their proposed model by using the acquired results for efficient data classification.

The paper entitled "IT governance and risk mitigation approach for private cloud adoption: case study of provincial healthcare provider" by Ayo Gbadeyan, Sergey Butakov, and Shaun Aghili looked into privacy issues in cloud computing, focusing on the Canadian healthcare industry[9]. The research presented a detailed IT governance and a risk mitigation approach for implementing cloud computing technologies. Specific areas for risk assessment in cloud computing deployment models were outlined and mapped to corresponding cloud architectural components. COBIT 5 was used as the main tool to propose risk mitigation in IT governance and management levels.

The paper entitled "Efficient designated server identity-based encryption with conjunctive keywords search" by Yang Lu, Gang Wang, Jiguo Li, and Jian Shen presents a cryptanalysis for Wu et al.'s proposed designated server identity-based encryption scheme with keyword search[10]. The cryptanalysis performed by the authors indicates that Wu et al.'s scheme fails in achieving ciphertext indistinguishability. They proposed and proved the improved scheme that satisfies ciphertext indistinguishability, trapdoor indistinguishability, and off-line keyword-guessing attack security.

The paper entitled "The three-dimensional model for dependability integration in cloud computing" by Wiem Abderrahim and Zied Choukair presents a model that integrates dependability with respect to three dimensions according to The Open Group Architecture Framework principles[11]. Their model proves an enhancement of dependability attributes compared to classically designed and executed cloud systems.

In conclusion, we would like to address our special thanks to Prof. Guy Pujolle, the Editor-in-Chief of *Annals of Telecommunications*, for his great support and efforts throughout the whole publication process of this special issue. We are also grateful to all the authors for submitting their papers and to the reviewers for their professional and timely work that helped us to select the best papers for publication. Our sincere thanks go to Nicolas Puech, the editorial staff especially Ms. Alexia Kappelmann and Ms. Véronique Charlet, and the Springer Journal Editorial Office for their continuous support to publish this special issue.

References

1. Somani G, Gaur MS, Sanghi D, Conti M, Buyya R (2016) Service resizing for quick DDoS mitigation in cloud computing environment. Ann Telecommun. doi:10.1007/s12243-016-0552-5

2. Amin R u, Inayat I, Shahzad B, Saleem K, Aijun L (2016) An empirical study on acceptance of secure healthcare service in Malaysia, Pakistan, and Saudi Arabia: a mobile cloud computing perspective. Ann Telecommun. doi:10.1007/s12243-016-0553-4
3. Farooqi AH, Khan FA (2017) Securing wireless sensor networks for improved performance in cloud-based environments. Ann Telecommun. doi:10.1007/s12243-017-0566-7
4. Sun Y, Wu L, Wu S, Li S, Zhang T, Zhang L, Xu J, Xiong Y, Cui X (2016) Attacks and countermeasures in the internet of vehicles. Ann Telecommun. doi:10.1007/s12243-016-0551-6
5. Nie L, Jiang D, Lv Z (2016) Modeling network traffic for traffic matrix estimation and anomaly detection based on Bayesian network in cloud computing networks. Ann Telecommun. doi:10.1007/s12243-016-0546-3
6. Mehak F, Masood R, Shibli MA, Elgedway I (2016) EACF: extensible access control framework for cloud Environments. Ann Telecommun. doi:10.1007/s12243-016-0548-1
7. Raza N, Rashid I, Awan FA (2017) Security and management framework for an organization operating in cloud environment. Ann Telecommun. doi:10.1007/s12243-017-0567-6
8. Jararweh Y, Al-Ayyoub M, Tawalbeh L'a, Darabseh A', Song H (2016) Software-defined systems support for secure cloud computing based on data classification. Ann Telecommun. doi:10.1007/s12243-016-0549-0
9. Gbadeyan A, Butakov S, Aghili S (2017) IT governance and risk mitigation approach for private cloud adoption: case study of provincial healthcare provider. Ann Telecommun. doi:10.1007/s12243-017-0568-5
10. Lu Y, Wang G, Li J, Shen J (2017) Efficient designated server identity-based encryption with conjunctive keywords search. Ann Telecommun. doi:10.1007/s12243-017-0574-7
11. Abderrahim W, Choukair Z (2017) The three-dimensional model for dependability integration in cloud computing. Ann Telecommun. doi:10.1007/s12243-017-0576-5