Editorial

Youness Tabii*, Mohammed Al Achhab and Mohamed Lazaar

Ecole Nationale des Sciences Appliquées de Tetouan (ENSA Tetuan),
BP: 2222 M'hannech, Morocco
Email: youness.tabii@gmail.com
Email: youness.tabii@uae.ma
Email: alachhab@gmail.com
Email: lazaarmd@gmail.com
*Corresponding author

Biographical notes: Youness Tabii received his PhD in July 2010 from the National School of Computer Sciences and Systems Analysis, Mohammed V University-Rabat. He is a Professor at the National School of Applied Sciences of Tetuan. He is a member in LIROSA Laboratory and the Head of Master: Embedded and Mobile Systems. His research interests include video processing and analysis and cloud security.

Mohammed Al Achhab received his PhD in the field of formal verification of reactive systems in December 2006 from the University of Franche-Comté, Besançon, France. He was a Temporary Lecturer and Research Assistant at the University of Franche-Comté from 2005 to 2006. He was an Assistant Professor at the Faculty of Sciences Dhar El Mehraz, Fez from 2007 to 2012. Currently, he is a Professor at the National School of Applied Sciences of Tetuan. His research focuses on analysis and validation of business process, and adaptive e-learning.

Mohamed Lazaar is a Professor of Computer Science at the National School of Applied Sciences of Tetuan in Morocco. Her main research areas include pattern recognition, neural network, genetics algorithm and algorithms of data mining.

Cloud computing has emerged as a popular computing model, with numerous advantages both to end users and providers. The obvious huge advantage is that customers can outsource their infrastructures and benefit of the best technologies and characteristics at low costs. The cost benefits offered by cloud technologies is one of the major reasons that stimulate the growth of cloud computing in many industries. In few years, cloud computing's acceptance from enterprises is increasing but businesses are now finding that there is a number of issues related to technology, resources, management, quality of service and security that have to be addressed when venturing into the cloud.

With fast growing in advance of big data science, analytics and technology, big data is a key enabler of exploring business insights, economics of services and help professionals to reduce risks with facilities to take decision.

BDCA '15 (Big Data, Cloud and Applications) created to provide an excellent meeting for researchers, industry and domain experts to exchange the latest advances in big data and cloud computing as well as their experience, knowledge and synergy.

BDCA'15 will be held at National School of Applied Sciences (ENSA), Tetuan, Morocco on May 25th and 26th 2015.

- The first paper entitled 'A broker framework for selecting secure cloud service provider using security risk approach', by Jamal Talbi and Abdelkrim Haqiq propose a broker framework that analyse and rank the cloud service providers based on measuring the risks of confidentiality, integrity and availability. This model uses a CSP rank framework for the group of cloud providers by assessing security metrics which make decision of the more secure provider among the available providers list and justify the business needs of users in terms of security and reliability.
- Second paper entitled 'Reinforce cloud computing access control with key policy attribute-based anonymous proxy reencryption', by Naîma Meddah and Ahmed Toumanari propose a fine-grained access control system using a combination of key-policy attribute-based encryption system and an anonymous proxy re-encryption. This proposed scheme is an efficient model that enforcing access policies based on data attributes, allowing the delegation of computation implicated in fine-grained access control to untrusted cloud servers without disclosing the data content. The proxy, however, learns nothing about the underlying plain-text. Key policy attribute-based encryption has many real world applications, such as fine-grained access control in cloud storage systems and medical records sharing among different hospitals. Previous schemes that use key policy attribute-based encryption and proxy re-encryption leave how to be secure against chosen-cipher-text attacks (CCA) as an open problem. The new scheme supports attribute-based encryption with anonymous proxy re-encryption, our construction enjoys the desirable properties of unidirectional, non-interactive, and multi-use, chosen cipher-text attacks and the secret key security is guaranteed.
- The third paper 'An enhanced approach for data sharing security in cloud computing', by Ibtissam Ennajjar, Youness Tabii and Abdelhamid Benkaddour. In this paper, authors give a new approach to enhance the security of data outsourced in cloud environment. The approach is based on cipher policy-attribute-based encryption (CP-ABE) scheme. It consists of encrypting data before outsourcing it and controlling the access to it by encryption. The proposed method offers scalability, flexibility and fine grained access control of data in cloud. Also, it provides an efficient manner to share confidential data on cloud servers.
- The last paper is 'Homomorphic encryption applied to secure storage and treatments of data in cloud', by Khalid El Makkaoui, Abdellah Ezzati and Abderrahim Beni Hssane. With the emergence of cloud computing, the concept of security has become a major issue. Indeed, the key challenge is to ensure to customers that the selected cloud provider may store and process the raw data in complete confidentiality. If this is a storage service, data can be encrypted before sending them to the cloud server; in this case, data confidentiality is assured. However, before performing treatments, these data must be decrypted. It is this step that can be considered a breach of confidentiality. Indeed, the fear of seeing sensitive data be processed in crude is a major obstacle in adopting cloud services. To overcome this obstacle and strengthen confidence in the cloud services, in this paper, authors propose an adoption of homomorphic encryption methods that are able to perform operations on encrypted data without knowing the key secret.