BIOMETRICS-AS-A-SERVICE: CLOUD-BASED TECHNOLOGY, SYSTEMS, AND APPLICATIONS

Silvio Barra
University of Cagliari

Kim-Kwang Raymond Choo
University of Texas at San Antonio

Michele Nappi
The University of Salerno

Arcangelo Castiglione
University of Salerno

Fabio Narducci
University of Naples "Parthenope"

Rajiv Ranjan
Newcastle University

The guest editors of the *IEEE Cloud Computing* special issue on Biometrics-as-a-Service discuss the benefits and challenges of using cloud computing with biometric authentication systems as well as the articles included in this issue. Three potential research topics are also discussed, including the use of machine/deep-learning techniques to circumvent existing biometric authentication solutions.

Interest and use of biometric authentication systems in cloud services continue to increase, partly because biometric credentials are harder to compromise in comparison to conventional password-based authentication. However, a number of challenges exist in deploying biometric authentication systems in cloud services (e.g. *function creep*-prone: gradual broadening of technology or system usage beyond the purpose for which it was originally intended). This special issue reports on state-of-the-art advances on this topic.

WHY THE NEED FOR BIOMETRICS IN THE CLOUD?

Cloud computing[1] is widely used in both scientific and business activities, as well as by individual users.[2] From the hardware infrastructure perspective, cloud computing helps to overcome

Copublished by the IEEE CS and IEEE ComSoc
2325-6095/18/$33.00 USD ©2018 IEEE

limitations in standalone computing. For example, organizations do not need to make significant investment in their computational processing and storage infrastructure, and can progressively scale up or down as needed. This drives down the cost in terms of hardware and ongoing maintenance supply, which is particularly crucial for small- and medium-sized organizations, and results in an entirely new ecosystem. For example, we now have organizations dedicated to the provision of infrastructure to manage cloud platforms and lease their resources to users based on their needs, and providers who pay for the rented resources from one or many infrastructure providers to serve other users.[3] Major cloud computing organizations include Google, Amazon, Microsoft, and Alibaba.

Challenges associated with the deployment and utilization of cloud services have been widely discussed in the literature. For example, ensuring the privacy of data while providing timely and secure access in a cloud computing environment, particularly in a federated or multi-cloud environment, can be extremely challenging.[4] This is partly due to differing privacy and related regulations and requirements on the management and storage of data between jurisdictions.[5,6] This necessitates the design of authentication system that ensures that data can only be accessed by authorized users.

Here, Biometrics-as-a-Service (BaaS) is a potentially attractive solution to providing ubiquitous authentication to cloud services. With BaaS, a service provider can offer a light way of accessing data, based on an individual's biometric traits (like fingerprint scanning or facial recognition); thus, mitigating potential fraudulent activities and streamlining customer service, without costly, time-consuming and resource-intensive software acquisition and integration processes. The potential for BaaS is also evidenced by recent services (i.e., biometric recognition to be used as a service on the cloud) offered by Fujitsu, BioID, ImageWare Systems, Animetrics, Aware and IriTech. Thus, this is the focus of this special issue.

Cloud-based biometric authentication (also referred to as biometrics-as-a-service) is a relatively new trend, replacing conventional password-based authentication system.[7] Using biometrics as a way of authentication on cloud computing architecture has potential benefits, such as scalability, cost-effectiveness, reliability, hardware agnostic, and allowing ubiquitous access to private data and services. In fact, biometric credentials have the advantage of not relying on the user's memory.

Existing biometric authentication literature generally focuses on how to acquire and/or process biometric traits for reliable recognition. Generally, biometric data (iris or face scan, fingerprint and so on) is captured during enrollment and converted into metadata (templates) for storage. User authentication takes place at a later stage by a matching process between the live acquired trait and previously stored template.

While biometric authentication systems offer a number of benefits over conventional password-based authentication systems, such systems are not perfect. For example, one's biometric traits cannot be replaced once they have been compromised. Hence, ensuring the secure storage of biometric traits is crucial but not sufficient, since biometric traits transmitted over public networks could be copied and exfiltrated by an eavesdropper. In addition, it has been demonstrated that using a fingerprint template rather than the original image does not guarantee the user's privacy.[8]

IN THIS SPECIAL ISSUE

The first contribution to this special issue, co-authored by Yang et al., is entitled "Tensor-based Big Biometric Data Reduction in Cloud," in which the authors proposed a biometric data tensor reduction solution for the cloud computing environment. Specifically, they model big biometric data using a tensor-based representation and use tensor decomposition techniques to achieve multidimensionality reduction of the big biometric data in the cloud.

The potential security and privacy challenges in cloud-connected mobile applications have been widely studied, and a number of solutions presented. Similarly, Fenu et al., in their article "Controlling User Access to Cloud-Connected Mobile Applications by Means of Biometrics," propose a continuous authentication approach, which integrates physical (face) and behavioral (touch and hand movements) biometrics to control user access to cloud-based mobile services.

De Marsico et al. present a smart peephole based on remote biometric services, in the article "House in the (biometric) cloud: a possible application." In their approach, minimal processing is carried out locally.

In the last article, entitled "Cognitive and Biometric Approaches to Secure Services Management in Cloud-Based Technologies," Ogiela et al. explain how different security procedures in data and service management can be applied in both the cloud and fog computing environments, as well as in distributed computing infrastructures. Service management in cloud computing has been presented in connection with secure cognitive management systems, supporting management tasks and securing important data using CAPTCHA solutions. All such protocols can use personal features and biometric patterns. Application of cognitive and biometric features allows the creation of personalized procedures, tailored for users or groups of participants who seek to gain access to particular data repositories or receive specific services. Furthermore, the use of these protocols allows new solutions in the area of user-oriented service management protocols to be developed.

CONCLUSIONS

While the articles in this special issue have contributed to the knowledge base on the topic, there are many more challenges that need to be addressed, such as those discussed by Popović and Hocenski.[9] For example,

1. Do we have solutions that assure us that when cloud service provider claims to have destroyed our biometric data, no copy of such data remains on their system?
2. Do we have solutions that allow us to know how and where our biometric data is stored at any point in time?
3. What about the secure storage of biometric traits?

Cryptosystems for biometrics can be broadly categorized into those that derive the key directly from the biometric trait acquired on-the-fly; and those that generate the key by binding the biometric trait and a random binary key. In both cases, the biometric trait does not need to be stored (except during enrolment when the acquired biometric data is used to generate the encrypted key). Once a user has been successfully enrolled, information from the acquired original biometric trait is no longer used or saved. However, when the biometric authentication takes place on cloud architectures, potential attacks to privacy may occur during the transmission of the acquired biometric trait through the network. For example, spoofing attacks can lead to identity theft,[10] which is particularly critical in biometrics due to the infeasibility of changing users' trait. A video recording or in some cases, a photograph of the authorized person, can be used to gain access to protected data. Thus, the interest in cancellable biometrics.[11,12] Cancellable biometrics refers to the systematic distortion applied intentionally on the original biometric image, with the aim of deriving a "new" trait used for authentication. In the event that the cancelable feature is compromised, a new distortion is applied on the original trait so that the same biometrics is mapped to a new template.

Potential research topic 1: To design a privacy-preserving computation framework, in order to handle robust and efficient biometrics fusion processing. This can facilitate situation-based identification and sharing in the cloud.

Potential research topic 2: To design solutions that can automatically scale or de-scale existing privacy preserving algorithms.

Potential research topic 3: To design machine/deep-learning based solutions that can be used to facilitate existing BaaS approaches.

ACKNOWLEDGEMENTS

We thank the authors for submitting their work to this special issue, the anonymous reviewers for providing constructive feedback, and Dr. Mazin Yousif, editor-in-chief of *IEEE Cloud Computing*, for his great support throughout the entire publication process.

REFERENCES

1. M. Armbrust et al., *Above the Clouds: A Berkeley View of Cloud Computing*, technical report Technical Report No. UCB/ EECS-2009-28, Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, 2009.
2. P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, National Institute of Standards and Technology, 2011.
3. Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the-art and research challenges," *Journal of Internet Services and Applications* (AICT 14), vol. 1, no. 1, 2014, pp. 7–18.
4. A. Castiglione et al., "Biometrics in the cloud: Challenges and research opportunities," *IEEE Cloud Computing*, vol. 4, no. 4, 2017, pp. 12–17.
5. A.J. Brown et al., "Cloud Forecasting: Legal Visibility Issues in Saturated Environments," *Computer Law & Security Review*, vol. In press, 2018; doi.org/10.1016/j.clsr.2018.05.031.
6. C. Hooper, B. Martini, and K.-K. R. Choo, "Cloud computing and its implications for cybercrime investigations in Australia," *Computer Law & Security Review*, vol. 29, no. 2, 2013, pp. 152–163.
7. S.C. Eastwood et al., "Biometric-enabled authentication machines: A survey of open-set real-world applications," *IEEE Transactions on Human-Machine Systems*, vol. 46, no. 2, 2016, pp. 231–242.
8. A. Ross, J. Shah, and A.K. Jain, "From template to image: Reconstructing fingerprints from minutiae points," *IEEE Transactions on Human-Machine Systems*, vol. 29, no. 4, 2007, pp. 544–560.
9. K. Popović and Ž. Hocenski, "Cloud computing security issues and challenges," *Proceedings of the 36th International Convention on Information and Communication Technology, Electronics and Microelectronics* (MIPRO 10), 2010, pp. 344–349.
10. N. Evans et al., "Guest editorial: Special issue on biometric spoofing and countermeasures," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, 2015, pp. 699–702.
11. V.M. Patel, N.K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Processing Magazine*, vol. 32, no. 5, 2015, pp. 54–65.
12. K.M.S. Soyjaudah, G. Ramsawock, and M.Y. Khodabacchus, "Cloud computing authentication using cancellable biometrics," *IEEE AFRICON*, 2013, pp. 1–4.

ABOUT THE AUTHORS

Silvio Barra is an assistant professor at the University of Cagliari and research collaborator at the Biometric and Image Processing Lab of the University of Salerno. He received BS and MS degrees cum laude at the University of Salerno in 2009 and 2012. In 2016, he received a PhD at the University of Cagliari. His research interests include biometric recognition, machine intelligence, and pattern analysis in images, signals and video. Contact him at silvio.barra@unica.it.

Kim-Kwang Raymond Choo holds the Cloud Technology Endowed Professorship in the Department of Information Systems and Cyber Security at the University of Texas at San Antonio. Choo has a PhD in information security from Queensland University of Technology. His research interests include cyber and information security and digital forensics. He is a senior member of IEEE, a Fellow of the Australian Computer Society, an Honorary

Commander, 502nd Air Base Wing, Joint Base San Antonio-Fort Sam Houston. Contact him at raymond.choo@fulbrightmail.org.

Michele Nappi is an associate professor of computer science at the University of Salerno and team leader of the Biometric and Image Processing Lab. His research interests include pattern recognition, image processing, image compression and indexing, multimedia databases and biometrics, human computer interaction, VR\AR. Nappi is an author of more than 160 papers in peer-reviewed international journals, international conferences and book chapters, and co-editor of several international books. He is an IEEE Senior Member, and president of the Italian Chapter of the IEEE Biometrics Council. Contact him at mnappi@unisa.it.

Arcangelo Castiglione is a post-doctoral fellow with the Department of Computer Science and an adjunct professor with the Department of Industrial Engineering at the University of Salern. He received a BS, MS, and PhD in computer science from the University of Salerno. His research mainly focuses on cryptography, multimedia data protection and network security. In 2015 he was a visiting researcher at the Laboratory of Cryptography and Cognitive Informatics at AGH University of Science and Technology, and at the School of Mathematics and Computer Science at Fujian Normal University. Contact him at arcastiglione@unisa.it.

Fabio Narducci is an assistant professor at the University of Naples "Parthenope," adjunct professor at the University of Molise, and research collaborator at the Biometric and Image Processing Lab of the University of Salerno. He received a PhD in computer science at the Virtual Reality Lab of the University of Salerno. His research interests include biometrics, gesture recognition, augmented reality, virtual environments, mobile and wearable computing, human computer interaction, haptics. Contact him at fabio.narducci@uniparthenope.it.

Rajiv Ranjan is a reader in the School of Computing Science at Newcastle University; chair professor in the School of Computer, Chinese University of Geosciences; and a visiting scientist at Data61, CSIRO. He has a PhD in computer science and software engineering from the University of Melbourne. Ranjan's research interests include grid computing, peer-to-peer networks, cloud computing, Internet of Things, and big data analytics. Contact him at raj.ranjan@ncl.ac.uk or http://rajivranjan.net.