

Received May 24, 2021, accepted May 24, 2021, date of current version June 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3084075

## COMMENTS AND CORRECTIONS

# Corrections to “Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry”

HINA ABRAR<sup>1</sup>, SYED JAWAD HUSSAIN<sup>2</sup>, JUNAID CHAUDHRY<sup>3,4</sup>, (Senior Member, IEEE),  
KASHIF SALEEM<sup>5</sup>, MEHMET A. ORGUN<sup>6</sup>, (Senior Member, IEEE),  
JALAL AL-MUHTADI<sup>5,7</sup>, AND CRAIG VALLI<sup>4</sup>

<sup>1</sup>Department of Computer Science and Engineering, HITEC University, Taxila 47120, Pakistan

<sup>2</sup>Department of Computer Science and Information Technology, The University of Lahore, Lahore 53710, Pakistan

<sup>3</sup>College of Security and Intelligence, Embry-Riddle Aeronautical University, Prescott, AZ 86305, USA

<sup>4</sup>Security Research Institute, Edith Cowan University, Joondalup, WA 6027, Australia

<sup>5</sup>Center of Excellence in Information Assurance, King Saud University, Riyadh 12372, Saudi Arabia

<sup>6</sup>Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

<sup>7</sup>College of Computer and Information Sciences, King Saud University, Riyadh 12372, Saudi Arabia

Corresponding author: Kashif Saleem (ksaleem@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research at King Saud University through the Research Group under Grant RG-1439-022.

In above article [1], reference [11] is incorrect as the conference article had not been published in full until 2019. The correct reference is cited here as [2]. Therefore, the sentences in the article [1] with reference [11] should be cited [2] in this article as “When the data are stored in a centralized location and are transmitted by applying symmetric data encryption techniques, the deployment and maintenance costs will go beyond cost tolerance thresholds [2],” “Since cloud computing signifies a comparatively novel computing representation at every level, like applications, hosts, network, and data, that in turn raises the issue of the application safety to shift toward cloud computing [2] and [3],” and “However, this definition is not accurate in the sense that, if the normal operation is susceptible to eavesdropping, in this case, the normal operation of the organization must be restricted [2].”

## REFERENCES

- [1] H. Abrar, S. J. Hussain, J. Chaudhry, K. Saleem, M. A. Orgun, J. Al-Muhtadi, and C. Valli, “Risk analysis of cloud sourcing in healthcare and public health industry,” *IEEE Access*, vol. 6, pp. 19140–19150, 2018, doi: 10.1109/ACCESS.2018.2805919.
- [2] J. Chaudhry, U. Qidwai, and M. H. Miraz, “Securing big data from eavesdropping attacks in SCADA/ICS network data streams through impulsive statistical fingerprinting,” in *Emerging Technologies in Computing (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering)*, vol. 285., M. Miraz, P. Excell, A. Ware, S. Soomro, and M. Ali, Eds. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-030-23943-5\_6.
- [3] D. G. Rosado, R. Gómez, D. Mellado, and E. Fernández-Medina, “Security analysis in the migration to cloud environments,” *Future Internet*, vol. 4, no. 2, pp. 469–487, May 2012.

...