Editorial for the Special Issue on Quality Assessment of Data Security

Due to rapid technical advancements, many devices such as sensors, embedded systems, actuators, and mobile/smart devices receive huge amounts of information through data exchange and interconnectivity. From this increase in the exchange of data, there has also been a direct correlation to sensitive information that also moves through systems continuously. In this context, it is critical to ensure that both private and personal data is not disclosed and that any confidential information can be successfully hidden. Therefore, security and privacy have attracted a great deal of attention in academia and industry in recent decades. Not only is there a reason to protect against data leakage that is sensitive in nature, but it is also imperative to ensure that users of such systems trust the means by which their data is exchanged.

Hundreds of security solutions have recently been discussed in the literature. However, the ability to properly manage the quality of security to ensure that developed models and algorithms can secure data is a very important task. To that end, only a limited number of works have addressed this problem directly. Since exchanged data usually is complex, researchers should also develop and investigate security models to perform quality assessments of data security. These tasks will ensure that threats from hackers or malware can be minimized.

Security solutions can take on many forms. From cryptographic primitives all the way to machine learning and artificial intelligence, these potential fail-safes need to be properly researched, disseminated and discussed to ensure the next generation of systems will adhere to certain standards in the realm of security and privacy.

This special issue saw a total of 21 submissions, from which five papers were published. It was intentional to adhere to a strict acceptance rate and ensure that only the best papers in the scope of the special issue were accepted. The following few paragraphs summarize the contributions that our special issue collection presents.

In "A Survey on Edge Intelligence and Lightweight Machine Learning Support for Future Applications and Services," Hoffpauir et al. provided a comprehensive survey of the emerging edge intelligence applications, lightweight machine learning algorithms, and their support for future applications and services. The survey started by analyzing the rise of cloud computing discussing its weak points, and identifying situations in which edge computing provides advantages over traditional cloud computing architectures. Then it dove into the survey - the first section identifying opportunities and domains for edge computing growth, the second identifying algorithms and approaches that can be used to enhance edge intelligence implementations, and the third specifically analyzing situations in which edge intelligence can be enhanced using any of the aforementioned algorithms or approaches. In this third section, lightweight machine learning approaches are detailed. A more in-depth analysis and discussion of future developments follow. The

ACM Reference format:
Gautam Srivastava, Jerry Chun-Wei Lin, and Zhihan Lv. 2023. Editorial for the Special Issue on Quality Assessment of Data Security. *ACM J. Data Inform. Quality* 15, 2, Article 19 (June 2023), 3 pages.
https://doi.org/10.1145/3591360

1936-1955/2023/06-ART19
https://doi.org/10.1145/3591360

primary discourse of this article is in an effort to ensure that appropriate approaches are applied adequately to artificial intelligence implementations in edge systems and mainly the lightweight machine learning approaches.

In "An Improved Encryption–Compression-based Algorithm for Securing Digital Images," Singh et al. developed an improved encryption-before-compression-based algorithm to secure digital images with minimal resource demands. The security assessment of the suggested solution was conducted in different ways, such as differential and statistical, key sensitivity, execution time, and perceptual quality analysis. The performed experimental analysis proved the method's security against various possible attacks at minimum overhead. Additionally, the evaluation of the image's perceptual quality indicated that the quality of the encrypted image reached a high level. Furthermore, extensive evaluations on a real dataset showed that the proposed solution is secure and has low encryption overhead compared to the other similar schemes.

In "A Survey on Soft Computing for Federated Learning-Applications, Challenges and Future Directions," Yarradodd et al. explored many interesting recent findings in the field of Federated Learning. **Federated Learning (FL)** is a distributed, data-private machine learning methodology that is currently gaining popularity. There are numerous uses for federated learning in various industries. Despite growing in popularity, it has many limitations, including high communication costs, privacy issues, and data management problems. The main focus of this work was on the issues with FL implementation and how various soft computing techniques can be used to solve them. The authors continued to research the effects of combining different nature-inspired methodologies with federated learning to address its shortcomings. The authors gave contributions and comparisons of Federated Learning and soft computing with previous works. The work briefly explains the fundamentals of distributed learning, federated learning, and an introduction to soft computing. Various soft computing techniques are explained individually in brief. Also, the work briefly dives into the motivation for integrating federated learning and soft computing. Applications of soft computing for FL explain the use of each nature-inspired algorithm in FL. Case studies of the duo are also consolidated, which is an added advantage to our work. Finally, this paper highlights potential future advancements in fusing soft computing with federated learning methods.

In "A Multifactor Ring Signature based Authentication Scheme for Quality Assessment of IoMT Environment in COVID-19 Scenario," Chatterjee et al. proposed a multifactor authentication scheme for a smart healthcare environment and also proposed measures to access the quality of the **Internet of Medical Things (IoMT)** environment. The various security proofs validate the claimed novelty of the proposal.

In "Experimental Evaluation of Covariates Effects on Periocular Biometrics: A Robust Security Assessment Framework," Kumar et al. proposed a periocular region-based biometric system and explores the effect of image quality covariates (artifacts) on the performance of periocular recognition. To simulate the real-time scenarios and understand the consequences of blur, resolution, and bit-depth of images on the recognition accuracy of periocular biometrics, the authors modelled out-of-focus blur, camera shake blur, low-resolution, and low bit-depth image acquisition using Gaussian function, linear motion, interpolation, and bit plane slicing. Experimental results showed that among all types of covariates, camera shake blur has less effect on the recognition performance, while out-of-focus blur significantly impacts it. Irrespective of image quality, the convolutional neural network produced excellent results, which proves the robustness of their developed model.

The editors would like to thank Andrea Marrella for his countless hours spent on this Special Issue as well as Senior Associate Editor Paolo Missier, and last but not least, Tiziana Catarci, current

Editor-In-Chief of ACM Journal of Data Information and Quality for responding to all queries and concerns raised by us as editors to ensure the Special Issue was an overwhelming success.

Gautam Srivastava
Brandon University (Canada)
srivastavag@brandonu.ca

Jerry Chun-Wei Lin
Western Norway University of Applied Sciences (Norway)
jerrylin@ieee.org

Zhihan Lv
Uppsala University (Sweden)
lvzhihan@gmail.com

Guest Editors