Guest Editorial Preface

Special Issue on Emerging Technologies for Security and Authentication of Electronic Health Record (EHR): Opportunities and Challenges

Shabir A. Parah, Post Graduate Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, Jammu and Kashmir

Irfan Mahmood, Department of Computer Engineering, Sejong University, Seoul, Republic of Korea

Mohammad Sajjad, Department of Computer Science, Islamia College University, Peshawar, Pakistan

With the exponential increase in the users of Internet and personal devices, we are witnessing an explosive growth of multimedia data on the Web. The excessively used networked infrastructure has resulted in electronics creeping into every important sphere of life, like banking, governance, commerce and healthcare etc., giving rise to e- banking, e- governance, e-commerce and e-healthcare (Kaw et al., 2018; Loan et al., 2017; Parah et al., 2018). Electronic-healthcare also referred to as e-health, is becoming very popular and is taking lead in healthcare related activities. E-healthcare is rapidly changing the dynamics of conventional paper-based healthcare and making the distance between a patient and doctor immaterial. However, successful implementation of an e-healthcare system is accompanied by a number of challenges at administrative as well as at technological level. One of the most important challenges that is faced by e-healthcare systems is the privacy and content authentication of Electronic Health Record (EHR) / Electronic Medical Record (EMR). Given the critical nature of patient information EMR/EHR needs highest degree of security the content should be properly authenticated. Though existing e-healthcare service providers claim that the patients can only access their electronic records; but in recent past a number of healthcare data intrusions and breaches have been reported in USA and various European countries (Healthcare IT News, 2017; Healthcare Informatics, 2018; Yaqoob et al., 2017; Norwich University Online, 2016); wherein medical data of millions of patients has been breached. Thus, there is a need of continuously upgrading the security standards for sensitive health data. The available methods for preserving the privacy of healthcare systems entirely trust the system operators. Therefore, the health-related information (EHR) is vulnerable to be exploited by even the authorized personnel in an immoral/unethical way and it is time to come up with solutions in this respect (Muhammad et al., 2016; Parah et al., 2018; Parah et al., 2017).

The aim of this special issue is to nurture novel and transformative frameworks for authentication and security of EHR taking into consideration the challenges in the current working scenario, where in Internet of Things (IoT) platforms and Cloud computing form an in separable part of e-health setups. This special issue also aims to nurture a research community committed to advancing research and education at the confluence of electronic patient data privacy, security and authentication. We had

received 24 papers and after a rigorous review we have accepted 6 for publication. The accepted papers and their main contributions are summarized as follows.

The first paper "Simulating Light-Weight-Cryptography Implementation for IoT Healthcare Data Security Applications' by Gutub et al., addresses the issues pertaining to the healthcare data shared using various portable devices within an IoT based setup. The authors present a light weight cryptographic solution for securing healthcare data. The second paper "Secure Framework for Internet of Things based e-Health System" by Bashir et al. The authors have focused upon secure transmission of EPR in an e-health system. In this regard a new security framework has been proposed where-in smart devices encrypt sensed physiological data with Light-Weight encryption algorithm and Advanced Encryption Standard cryptographic algorithms. The security framework and the designed protocol have been proved to provide better security and are have been shown to be energy efficient. The third paper by Giri et al., presents a discrete wavelet based watermarking scheme for authentication of medical images. The authors have proposed a watermarking scheme for authentication of medical images. The scheme has been proved to be robust against various common image processing attacks. In the fourth paper entitled 'Experimental evaluation of a secure and ubiquitous architecture for electronic health records retrieval' the authors propose that pervasive and ubiquitous computing is a better way to manage EHR systems. An extended experimental evaluation of a secure architecture based on ubiquitous computing for medical records has been carried out to validate the claim. The last two papers pertain to privacy of healthcare data when Cloud services are used for security of such data. The papers discuss the challenges and solutions to ensure that the data is not intruded by the Cloud administrators.

The papers presented in this special issue are closely related to its theme and address the security and authentication issues for the EPR/EHR in e-health systems. We are sincerely hopeful that this special issue would appeal to both the experts as well as budding research scholars in the area and prove as an important platform to take the research in the field of EHR/EMR security and authentication forward. We are highly grateful to the contributing authors for their valuable contributions, and worthy reviewers for their time to make this issue a success. We would also like to thank the editor in chief of IJEHMC, Prof. Joel Rodriquez, and the entire editorial staff for their support their kind support and help during the entire process of publication.

Shabir A. Parah
Irfan Mahmood
Mohammad Sajjad
Guest Editors
IJEHMC

REFERENCES

Healthcare I.T. News. (n.d.). The biggest healthcare breaches of 2017. Retrieved from https://www.healthcareitnews.com/slideshow/biggest-healthcare-breaches-2017-so-far?page=8

Healthcare Informatics. (n.d.). 4.4M Patient Records Breached in Q3 2018, Protenus Finds. Retrieved from https://www.healthcare-informatics.com/news-item/cybersecurity/44m-patient-records-breached-q3-2018-protenus-finds

Kaw, J. A., Loan, N. A., Parah, S. A., Muhammad, K., Sheikh, J. A., & Bhat, G. M. (2018). A reversible and secure patient information hiding system for IoT driven e-health. *International Journal of Information Management*. doi:10.1016/j.ijinfomgt.2018.09.008

Loan, N. A., Parah, S. A., Sheikh, J. A., Akhoon, J. A., & Bhat, G. M. (2017). Hiding Electronic Patient Record (EPR) in medical images: A high capacity and computationally efficient technique for e-healthcare applications. *Journal of Biomedical Informatics*, *73*, 125–136. doi:10.1016/j.jbi.2017.08.002 PMID:28782602

Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S. W. (2016). A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. *Multimedia Tools and Applications*, *75*(22), 14867–14893. doi:10.1007/s11042-015-2671-9

Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S. W. (2016). Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. *Future Generation Computer Systems*. doi:10.1016/j.future.2016.11.029

Norwich University Online. (n.d.). Healthcare Data Breaches - The Costs and Solutions. Retrieved from https://online.norwich.edu/academic-programs/masters/nursing/resources/infographics/healthcare-data-breaches-the-costs-and-solutions

Parah, S. A., Sheikh, J. A., Akhoon, J. A., & Loan, N. A. (2018). Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication. *Future Generation Computer Systems*. doi:10.1016/j.future.2018.02.023

Parah, S. A., Sheikh, J. A., & Bhat, G. M. (2017). StegNmark: A joint stego-watermark approach for early tamper detection. In *Intelligent techniques in signal processing for multimedia security* (pp. 427–452). Cham: Springer. doi:10.1007/978-3-319-44790-2_19

Parah, S. A., Sheikh, J. A., Loan, N. A., Ahad, F., & Bhat, G. M. (2018). Utilizing neighborhood coefficient correlation: A new image watermarking technique robust to singular and hybrid attacks. *Multidimensional Systems and Signal Processing*, *29*(3), 1095–1117. doi:10.1007/s11045-017-0490-z

Yaqoob, I., Ahmed, E., Rehman, M. H., Ahmed, A. I. A., Al-Garadi, M. A., Imran, M., & Guizani, M. (2017, December). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, *129*(Part 2), 444–458. doi:10.1016/j.comnet.2017.09.003