Wireless Personal Communications (2021) 117:1–6
https://doi.org/10.1007/s11277-021-08104-z

EDITORIAL

# Reliable and Secure e-Health Networks

**Homero Toral-Cruz[1] · Debiao He[2] · Albena D. Mihovska[3] · Kim-Kwang Raymond Choo[4] · Muhammad Khurram Khan[5]**

Published online: 3 February 2021


Electronic health (e-health) is becoming a norm in our society, particularly in the current COVID-19 pandemic. Consequently, the volume, variety, velocity and veracity of healthcare data are also increasing. Due to the nature of healthcare data (e.g., patient's medical history and diagnosis), e-health network reliability and security are crucial. While e-health network reliability and security have been the focus of research in recent years, many open research issues remain, particularly as technologies advance. For example, traditional security strategies may not have kept pace with advances in e-health technologies and societal requirements (e.g., increasing privacy regulations). Thus, this special issue presents various state-of-the-art advances and research opportunities on the topics of e-health network reliability and security, covering both theoretical and practical aspects.

Specifically, in this special issue twelve (12) research papers were accepted after several rounds of reviews, based on their originality, quality, and merit.

The first paper by Pandey et al. [1] presents a solution to detect and thwart the circulation of counterfeit medicines in India through resilient electronic health networks

✉ Homero Toral-Cruz
htoral@uqroo.edu.mx

Debiao He
hedebiao@whu.edu.cn

Albena D. Mihovska
amihovska@btech.au.dk

Kim-Kwang Raymond Choo
raymond.choo@fulbrightmail.org

Muhammad Khurram Khan
mkhurram@ksu.edu.sa

[1] Department of Sciences and Engineering, University of Quintana Roo, Boulevard Bahía s/n Esq. Ignacio Comonfort, Col. del Bosque, 77019 Chetumal, Quintana Roo, México

[2] School of Cyber Science and Engineering, Wuhan University, Wuchang, Wuhan 430072, Hubei, China

[3] Department of Business Development and Technology, Aarhus University, Birk Centerpark 15, Building 8001, Innovatorium, CGC, 7400 Herning, Denmark

[4] Department of Information Systems and Cyber Security, University of Texas at San Antonio, 1 UTSA Cir, San Antonio, TX 78249, USA

[5] Center of Excellence in Information Assurance, King Saud University, Po Box 92144, Riyadh 11653, Kingdom of Saudi Arabia

using blockchain. To achieve this, the authors proposed recording the medicine logistics requirements from medicine manufacturing to the patient on the blockchain. The system is simulated using a decentralized network of eleven computer nodes and its performance is compared with other existing methods under different network configurations. The authors' simulation results showed that the system offers a reliable solution to the menace of fake medicines.

The second paper by Kumari et al. [2] proposes improvements to the scheme recently presented by Qiu et al. designed for telecare medical information systems (TMIS). The authors show that Qiu et al.'s protocol is vulnerable to offline password guessing, replay, and anonymity violation attacks. To avoid these weaknesses, the authors developed an improved biometric-based three-factor protocol with added security features. The authors claimed that the proposed protocol is more secure and efficient as compared with other authentication protocols for the healthcare environment. To validate this, they use Burrows–Abadi–Needham (BAN) logic.

The third paper by Alzahrani et al. [3] proposes improvements to the new patient healthcare monitoring and authentication protocol presented by Xu et al., designed for WBAN environments. The authors showed that Xu et al.'s protocol is vulnerable to many attacks, including replay attacks and key compromise impersonation attacks, and that it suffers from privacy issues. To avoid these shortcomings, the authors proposed an improved scheme and formally analyzed its security features by implementing BAN logic and an automated simulation tool.

The fourth paper by Xie et al. [4] presents a basic RFID authentication protocol for the healthcare environment, based on indistinguishability obfuscation, to prevent the leakage of sensitive data from the backend server. They claimed that their proposed protocol is the first applications of indistinguishability obfuscation in the field of RFID authentication system, as well as being scalable.

The fifth paper by Chauhan et al. [5] presents an integrated framework of big data analytics with privacy and security concerns in context with healthcare databases for patients suffering from Human Immunodeficiency Virus (HIV) and Tuberculosis (TB). The proposed framework focuses on the detection of patterns from healthcare databases and generation of patterns for future clinical decision making. Finally, the authors proposed a framework using unsupervised learning techniques in STATA and MATLAB 7.1 to develop patterns for the knowledge discovery process. The authors emphasized that their study can potentially benefit end-users to predict future prognosis of the disease and combinatorial effects in determining varied policies that can assist patients with needs.

The sixth paper by Memos et al. [6] proposes a cloud infrastructure for e-health data transmission. In this paper, the authors redesigned the cloud computing model to support better resource allocation, less analysis time of the users' files and quicker response to the users' requests to the cloud servers. They proposed a cloud model architecture comprising four layers: (a) the master cloud server, (b) the slave servers, (c) the virtual sub servers and (d) the users connected to the cloud. The authors' experimental results showed that the proposed layered cloud architecture is more lightweight, efficient, and secure for e-health data transmission.

The seventh paper by Goyal et al. [7] presents a posture aware dynamic data delivery (PA-DDD) protocol in WBAN to deal with shadow effect due to body movement and change in posture. To avoid this problem, the authors used an Improved Initial Centroid K-means (IIC K-means) clustering technique for classification of various human body postures followed by back propagation neural network as a classifier to recognize human body

posture. The authors' simulation results showed that the proposed protocol prolongs the network lifetime and is energy efficient.

The eighth paper by Rachata et al. [8] proposes a mobile application to provide an efficient self-monitoring, which can encourage patients with type 2 diabetes mellitus and hypertension to improve their health status for preventing themselves from cardiovascular complication. To demonstrate the progression of the health status for the patients, the authors used the trend progression module, modelled with a fuzzy logic-based method. To verify an accuracy of the proposed mobile application, the authors tested one hundred twenty-one patients with type 2 diabetes mellitus and hypertension. Finally, the authors showed that the developed mobile application obtains 92% trend progression accuracy compared with decisions from eleven healthcare professionals and can encourage 85% of patients to improve their health status.

The ninth paper by Boubiche et al. [9] reviews the most leading protocols and classify them based the addressed security issue in the wireless sensor networks (WSN). In this paper, the authors outlined the main security constraints and challenges and present the future research directions based on the emerged application fields.

The tenth paper by Chaising et al. [10] proposes the personalized recommendation method using integrated objective distance for preventing Cardiovascular Disease (CVD) complication in the elderly. The authors' experimental results showed that the proposed new measurement can efficiently compute the shortest objective distance between the current health status of elderly individuals and the expected objective level. To verify the proposed model's accuracy, the authors compared the recommendations for 121 elderly persons with the high risk of developing this critical disease with expert recommendations. Finally, the authors showed that the proposed new approach has a high ability in providing personalized recommendation, which is nearly identical to the expert with 95% accuracy.

The eleventh paper by Goyal et al. [11] presents a hybrid Genetic Algorithm (GA) with BAT and Transmission Rate Adaption Policy (TRAP) abbreviated GABAT-TRAP to maximize the energy efficiency of the Wireless Body Area Networks (WBAN) with consideration of both the limitations of Quality of Service (QoS) metrics and dynamic link properties. The authors' simulation results showed that the proposed scheme improves the energy efficiency of WBAN without violating the QoS parameters such as packet delivery ratio, packet loss rate (PLR), and throughput as compared to other schemes such as TRAP, GA-TRAP, BAT-TRAP, UPA, TPC, and LSEPC.

The twelfth paper by Soldatos et al. [12] proposes a platform called SecureIoT to provide security monitoring, security analysis and security automation functionalities on IoT applications that involve smart objects. The authors claimed that the proposed platform enables the collection and analysis of security information from all elements of an IoT systems, including field, edge, and cloud elements. In addition, it allows for the flexible integration of different machine learning and AI models based on the modular and powerful mechanism of IoT security templates. To validate the functionalities, the authors used an Ambient Assisted Living (AAL) system that comprises socially assistive robots.

Now that we have summarized all accepted papers, we would like to thank the Editor-in-Chief (Professor Ramjee Prasad), Mr. Meertinus Faber (Project Coordinator) and Mr. Joseph Ian Reyes (Journal's Editorial Office Assistant) for their support, assistance and for giving us the opportunity to realize this special issue. We also would like to sincerely thank all the authors for their contributions and the subject matter experts for their time and efforts in reviewing the submissions to this special issue. We hope you will enjoy reading this special issue.

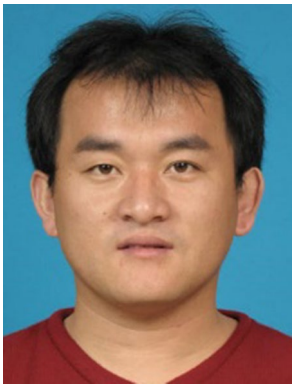
## References


1. Pandey, P., & Litoriya, R. (2020). Securing e-health networks from counterfeit medicine penetration using blockchain. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07041-7.
2. Kumari, S., & Renuka, K. (2019). Design of a password authentication and key agreement scheme to access e-healthcare services. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-019-06755-7.
3. Alzahrani, B. A., Irshad, A., Albeshri, A., et al. (2020). A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07237-x.
4. Xie, S., Zhang, F., & Cheng, R. (2020). Security enhanced RFID authentication protocols for healthcare environment. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07042-6.
5. Chauhan, R., Kaur, H., & Chang, V. (2020). An optimized integrated framework of big data analytics managing security and privacy in healthcare data. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07040-8.
6. Memos, V. A., Psannis, K. E., Goudos, S. K., et al. (2019). An enhanced and secure cloud infrastructure for e-health data transmission. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-019-06874-1.
7. Goyal, R., Patel, R. B., Bhaduria, H. S., et al. (2019). An efficient data delivery scheme in WBAN to deal with shadow effect due to postural mobility. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-019-06997-5.
8. Rachata, N., & Temdee, P. (2020). Mobile-based self-monitoring for preventing patients with type 2 diabetes mellitus and hypertension from cardiovascular complication. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07440-w.
9. Boubiche, D. E., Athmani, S., Boubiche, S., et al. (2020). Cybersecurity issues in wireless sensor networks: current challenges and solutions. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07213-5.
10. Chaising, S., Prasad, R., & Temdee, P. (2019). Personalized recommendation method for preventing elderly people from cardiovascular disease complication using integrated objective distance. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-019-06639-w.
11. Goyal, R., Patel, R. B., Bhaduria, H. S., et al. (2020). An energy efficient QoS supported optimized transmission rate technique in WBANs. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07281-7.
12. Soldatos, J., Kyriazakos, S., Ziafati, P., et al. (2020). Securing IoT applications with smart objects: framework and a socially assistive robots case study. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07039-1.




**Homero Toral-Cruz** received his PhD and MS degrees in Electrical Engineering, Telecommunication option from Center for Research and Advanced Studies of the National Polytechnic Institute (CINVESTAV), Jalisco, Mexico, in 2010 and 2006, respectively. He received his BSc degree in Electronic Engineering from "Instituto Tecnológico de la Laguna", Coahuila, Mexico in 2002. He is currently an assistant professor at Sciences and Engineering department at the University of Quintana Roo, Mexico. Prior to holding this position, he served as an assistant researcher at Electrical Engineering department, Telecommunication section in CINVESTAV, Jalisco, Mexico. His research interest includes network measurement, IP technologies, network security and wireless sensor networks. He has served as guest editor of some high quality journals. In addition, he has served as a chair, organizing committee member and technical program committee member for many international conferences and workshops. Dr Toral is also an active reviewer of some renowned international journals. Furthermore, he has been awarded a national recognition as a

researcher (SNI level 1) by CONACYT and has been elected as member of the Mexican Academy of Sciences (AMC).



**Debiao He** received his Ph.D. degree in applied mathematics from School of Mathematics and Statistics, Wuhan University, Wuhan, China in 2009. He is currently a professor of the School of Cyber Science and Engineering, Wuhan University, Wuhan, China. His main research interests include cryptography and information security, in particular, cryptographic protocols. He has published over 150 research papers in refereed international journals and conferences, such as IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Security and Forensic, and Usenix Security Symposium. He is the recipient of the 2018 IEEE Systems Journal Best Paper Award and the 2019 IET Information Security Best Paper Award. His work has been cited more than 7000 times at Google Scholar. He is on the Editorial Board of several international journals, such as Journal of Information Security and Applications, Frontiers of Computer Science, and Human-centric Computing & Information Sciences.

**Albena D. Mihovska** obtained the Ph.D. from Aalborg University, Denmark, where she was as an Associate Professor at the Center for TeleInfrastruktur (CTIF), Aalborg University. Currently, Dr. Albena is working as an Associate Professor in the Department of Business Development and Technology, School of Business and Social Sciences, Aarhus University (Denmark) since January, 2017, where she is presently involved on several European and Internal projects. She has close to two decades experience as a researcher in the area of mobile telecommunication systems. She was deeply involved in the design of a next generation radio communication system through her work as the AAU research team leader in the FP6 European funded project WINNER and WINNER II, and later continuing under the CELTIC framework programme as WINNER+, with the related research laying most of the foundations for the current Long-Term Evolution (LTE) and LTE-Advanced, the latter approved as an IMT-Advanced standard in ITU-Radio Sector. She has conducted research activities within the area of advanced radio resource management, cross-layer optimization, and spectrum aggregation, the results of which were put forward as IMT-A standardization proposals to the Radio Communication Study Groups of the ITU by the WINNER+ Evaluation Group. She has more than 100 research publications including 5 books in the next generation mobile communication systems. Further, one of her papers on the topic of next generation communication systems was voted at number 51 of the top 100 IEEE papers for July 2009. She is actively involved in ITU-T Standardization activities within SG13, and Focus Groups Cloud Computing, Smart Grids. She is also actively involved within IEEE Smart Grid Activities. She is a Steering Committee Member of IEEE WCNC, Special Session Chair of GWS2014, and Program Committee CoChair for the Wireless Telecommunication Symposium (WTS) 2015. She was Publicity Chair for WPMC2002, Treasurer of IEEE WCNC2006, Secretary of IEEE ComSoc WiMAX 2009 and on the TPC of many highly renowned international conferences, such as IEEE ICC, IEEE VTC, and so forth. She is an Associate Editor of the Inder-Science International Journal of Mobile Network Design and Innovation (IJMNDI).

**Kim-Kwang Raymond Choo** received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). He is an IEEE Computer Society Distinguished Visitor from 2021 to 2023, included in Web of Science's Highly Cited Researcher in the field of Cross-Field – 2020, named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn) in 2016, and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2019 IEEE Technical Committee on Scalable Computing (TCSC) Award for Excellence in Scalable Computing (Middle Career Researcher), the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, the Outstanding Associate Editor of 2018 for IEEE Access, the British Computer Society's 2019 Wilkes Award Runner-up, the 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, the Fulbright Scholarship in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award in 2008. He has also received best paper awards from the IEEE Consumer Electronics Magazine in 2020, EURASIP Journal on Wireless Communications and Networking (JWCN) in 2019, IEEE TrustCom 2018, and ESORICS 2015; the Korea Information Processing Society's Journal of Information Processing Systems (JIPS) Survey Paper Award (Gold) 2019; the IEEE Blockchain 2019 Outstanding Paper Award; and Best Student Paper Awards from Inscrypt 2019 and ACISP 2005.

**Muhammad Khurram Khan** is currently working as a Professor of Cybersecurity at the Center of Excellence in Information Assurance, King Saud University, Kingdom of Saudi Arabia. He is founder and CEO of the 'Global Foundation for Cyber Studies and Research' (http://www.gfcyber.org), an independent and non-partisan cybersecurity think-tank in Washington D.C, USA. He is the Editor-in-Chief of 'Telecommunication Systems' published by Springer-Nature with its recent impact factor of 1.73 (JCR 2020). He is on the editorial board of several journals including, IEEE Communications Surveys & Tutorials, IEEE Communications Magazine, IEEE Internet of Things Journal, IEEE Transactions on Consumer Electronics, Journal of Network & Computer Applications (Elsevier), IEEE Access, IEEE Consumer Electronics Magazine, PLOS ONE, and Electronic Commerce Research, etc. He has published more than 380 papers in the journals and conferences of international repute. In addition, he is an inventor of 10 US/PCT patents. He has edited 10 books/proceedings published by Springer-Verlag, Taylor & Francis and IEEE. His research areas of interest are Cybersecurity, digital authentication, IoT security, biometrics, multimedia security, cloud computing security, cyber policy, and technological innovation management. He is a fellow of the IET (UK), a fellow of the BCS (UK), and a fellow of the FTRA (Korea). He is the Vice Chair of IEEE Communications Society Saudi Chapter. He is a distinguished Lecturer of the IEEE. His detailed profile can be visited at http://www.professorkhurram.com.